BOUNDS ON ORDERED CODES AND ORTHOGONAL ARRAYS

ALEXANDER BARG* AND PUNARBASU PURKAYASTHA†

ABSTRACT. We derive new estimates of the size of codes and orthogonal arrays in the ordered Hamming space (the Niederreiter-Rosenbloom-Tsfasman space). We also show that the eigenvalues of the ordered Hamming scheme, the association scheme that describes the combinatorics of the space, are given by the multivariate Krawtchouk polynomials, and establish some of their properties.

CONTENTS

1. INTRODUCTION

1-A. **The Niederreiter-Rosenbloom-Tsfasman metric space.** Let $\mathcal{Q}$ be a finite alphabet of size q viewed as an additive group mod q. Consider the set $\mathcal{Q}^{r,n}$ of vectors of dimension rn over $\mathcal{Q}$. A vector $\boldsymbol{x}$ will be written as a concatenation of n blocks of length r each, $\boldsymbol{x} = \{x_{11}, \dots, x_{1r}; \dots ; x_{n1}, \dots, x_{nr}\}$. For a given vector $\boldsymbol{x}$ let $e_i, i = 1, \dots, r$ be the number of r-blocks of $\boldsymbol{x}$ whose rightmost nonzero entry is in the ith position counting from the beginning of the block. The r-vector $e = (e_1, \dots, e_r)$ will be called the *shape*

Key words and phrases. Ordered Hamming space, association schemes, multivariate Krawtchouk polynomials, Delsarte method, asymptotic bounds.

Date: July 10, 2009. *AMS Subject Classification*: Primary 05E30, Secondary 94B65. Research supported in part by NSF grants CCF0515124 and CCF0635271, and by NSA grant H98230-06-1-0044.

* Dept. of Electrical and Computer Engineering and Institute for Systems Research, University of Maryland, College Park, MD 20742, USA, and Institute for Problems of Information Transmission, Russian Academy of Sciences, Moscow, Russia. Email: abarg@umd.edu.

† Dept. of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742. Email: ppurka@umd.edu.

of $\boldsymbol{x}$. For two vectors $\boldsymbol{x},\boldsymbol{y}\in\mathcal{Q}^{r,n}$ let us write $\boldsymbol{x}\sim_e\boldsymbol{y}$ if $\operatorname{shape}(\boldsymbol{x}-\boldsymbol{y})=e$. A shape vector $e=(e_1,\dots,e_r)$ defines a partition of a number $N\le n$ into a sum of r parts. Let $\Delta_{r,n}=\{e\in(\mathbb{Z}_+\cup\{0\})^r:\sum_i e_i\le n\}$ be the set of all such partitions. For brevity we write

$$|e|=\sum_i e_i,\quad |e|'=\sum_i ie_i,\quad e_0=n-|e|.$$

Let $\boldsymbol{x}\in\mathcal{Q}^{r,n}$ be a vector of shape e. Define a weight function (norm) on $\mathcal{Q}^{r,n}$ by setting $\mathrm{w}(\boldsymbol{x})=|e|'$ and let $d_r(\boldsymbol{x},\boldsymbol{y})=\mathrm{w}(\boldsymbol{x}-\boldsymbol{y})$ denote the metric induced by this norm. We call the function d_r the *ordered weight*. The ordered weight was first introduced by Niederreiter [29] in his study of low-discrepancy point sets. Later, Rosenbloom and Tsfasman [34] independently defined the weight $\mathrm{w}(\boldsymbol{x})$ (more precisely, the weight $\bar{\mathrm{w}}$ defined below), calling it the m-metric, and studied codes in $\mathcal{Q}^{r,n}$ with respect to it. The set $\mathcal{Q}^{r,n}$ together with this metric will be called the *ordered Hamming space* (the *NRT space*) and denoted by $\overrightarrow{H}=\overrightarrow{H}(q,n,r)$. Unless specified otherwise, below by distance (weight) we mean the ordered distance (weight) for some fixed value of r. Note that the case $r=1$ corresponds to the usual Hamming distance on $\mathcal{Q}^n$.

An (nr,M,d) *ordered code* $C\subset\mathcal{Q}^{r,n}$ is an arbitrary subset of M vectors in $\mathcal{Q}^{r,n}$ such that the ordered distance between any two distinct vectors in C is d or more. If $\mathcal{Q}$ is a finite field and C is a linear code of dimension k, we refer to it as an $[nr,k,d]$ code.

To define ordered orthogonal arrays, let us call a subset of coordinates $\mathcal{I}\subset\{1,\dots,rn\}$ *left-adjusted* if with any coordinate $ir+j, 0\le i\le n-1, 1\le j\le r$ in the ith block it also contains all the coordinates $(ir+1,\dots,ir+j-1)$ of the same block. A subset $A\subset\mathcal{Q}^{r,n},|A|=M$ is called a (t,n,r,q) *ordered orthogonal array* (OOA) of strength t if its projection on any left-adjusted set of t coordinates contains all the q^t rows an equal number, say θ, of times. The parameter θ is called the *index* of A. It follows that $M=\theta q^t$. If C is a linear $[nr,k,d]$ code then the code orthogonal to it with respect to the dot product is a $(d-1,n,r,q)$ linear OOA of index $\theta=q^{nr-k-d+1}$. If $\mathcal{Q}$ is equipped with the structure of an additive group, then one can construct *additive* OOAs. If $\mathcal{Q}$ is a finite field, it is possible to construct linear OOAs.

OOAs (also called hypercubic designs) were introduced in Lawrence [20] and Mullen and Schmid [28] as a combinatorial equivalent of point sets suitable for numerical integration over the cube. Informally this link can be described as follows. Let $C_n=[0,1]^n$ be a unit cube, let f be a continuous function of bounded variation and let $\mathcal{N}$ be a set of $M=q^m$ points in C_n, called a net. It is known that the error of quasi-Monte Carlo integration $|\int_{C_n}fdx-q^{-m}\sum_{x\in\mathcal{N}}f(x)|$ can be bounded above by $V(f)D(\mathcal{N})$ where $V(f)$ is the total variation of f on C_n and $D(\mathcal{N})$ is the discrepancy factor of the net. The parameter $D(\mathcal{N})$ measures the deviation of the net from a uniformly distributed set of points. The study of uniformly distributed point sets was initiated by H. Weyl and E. Hlawka. Sobol [36] developed the notions described above and gave the first constructions of nets with bounded factor D. The study of nearly uniform point sets was taken up in Niederreiter [29] which put forward the notion of (t,m,s)-nets and derived a bound on $D(\mathcal{N})$ via its parameters. We refer to [23, 31, 30] for detailed background and more references for (t,m,s)-nets and in particular, to the literature on their constructions.

The following theorem relates OOAs and (t,m,s)-nets. Below we use its statement as a definition of a (t,m,s)-net.

Theorem 1.1. (Lawrence [20], Mullen and Schmid [28]). *There exists a (t,m,s)-net if and only if there exists an $(m-t,s,m-t,q)$ OOA of index q^t and size $M=q^m$.*

Independently of this line of work, Rosenbloom and Tsfasman [34] considered codes in the ordered Hamming space and derived bounds on their size. It became clear shortly after their work that OOAs and ordered codes are dual types of objects in the sense of Delsarte's algebraic theory of coding. This link opened up an avenue for applications of coding-theoretic methods to the study of (t, m, s)-nets and motivated the study of ordered codes and OOAs independently of these applications. In particular, Martin [24, 25, 22, 26] has constructed an association scheme that describes the combinatorics of the space $\overrightarrow{H}$, formulated the linear programming bound (LP bound), outlined a construction of orthogonal polynomials that describe the eigenvalues of the scheme and derived Plotkin and Rao bounds on OOAs via linear programming. Much attention was also devoted to relations between the weight enumerators of linear codes and their duals in the ordered Hamming space and its generalizations. In particular, a MacWilliams theorem for the NRT space was derived by Martin [24], see also Skriganov [35], Dougherty and Skriganov [14]. Bierbrauer [8, 9, 10] studied coding constructions of (t, m, s)-nets and bounds for them including the LP bound. Apart from the combinatorial context, ordered codes arise in a number of applied problems such as recent algebraic list decoding algorithms of Reed-Solomon codes [32], a study of linear complexity of sequences [27], and in a problem in communication theory [16].

In this paper, we derive several new bounds on OOAs and ordered codes. We begin with a Bassalygo-Elias bound on codes which improves the known upper bounds on their size. However, the bulk of our results are devoted to code bounds using the approach via association schemes and linear programming. We begin with a study of the eigenvalues of the ordered Hamming scheme, an association scheme that describes the combinatorics of the space $\overrightarrow{H}$. The approach that we follow relies on the orthogonality relation of the eigenvalues. This enables us to identify the eigenvalues as multivariate generalizations of the well-known Krawtchouk polynomials, i.e., a family of real polynomials of r discrete variables orthogonal on $\Delta_{r,n}$ with respect to the weight given by the multinomial probability distribution. This is the subject of Section 3. Turning to bounds, in Sect. 5 we derive a new universal estimate of the size of ordered codes and OOAs with a given distance (strength). The asymptotic version of this estimate improves the other results in a certain range of rates. The final section is devoted to the case $r = 2$ for which the bounds can be further improved relying on a direct approach.

1-B. **Notation.** Together with the space $\overrightarrow{H}$ we will consider the space $\overleftarrow{H}(q, n, r)$ which differs from it in that the vectors are read "from right to left." Namely, for $\boldsymbol{x} \in \mathcal{Q}^{r,n}$ let $\overline{\text{shape}}(\boldsymbol{x}) = (e_1, \dots, e_r)$, where e_j is the number of blocks $(x_{i1}, \dots, x_{ir})$ such that $x_{i1} = \cdots = x_{i,r-j} = 0$ and $x_{i,r-j+1} \neq 0$. Let $\bar{\text{w}}(\boldsymbol{x}) = |e|'$, where $e = \overline{\text{shape}}(\boldsymbol{x})$, and let $\bar{d}_r(\boldsymbol{x}, \boldsymbol{y}) = \bar{\text{w}}(\boldsymbol{x} - \boldsymbol{y})$.

These metric spaces are identical to each other; the reason for considering them both is that if we equip $\overrightarrow{H}$ with the structure of an association scheme then its dual scheme in Delsarte's sense gives rise to the space $\overleftarrow{H}$. In particular, if $\mathcal{Q}$ is a finite field and C is a linear code in $\overrightarrow{H}$ then its dual code $C^\perp$ lives in $\overleftarrow{H}$. We elaborate on this below.

An easy combinatorial calculation shows that the number of vectors of shape e in $\overrightarrow{H}$ is given by

$$v_e = \binom{n}{e_0, e_1, \dots, e_r} (q-1)^{|e|} q^{|e|' - |e|} \tag{1}$$

and the number of vectors of weight d equals to

$$S_d = \sum_{e:|e|'=d} v_e. \tag{2}$$

Let $A(z) = (q-1)z(z^r-1)/(q(z-1))$ and let $z_0 = z_0(x)$ satisfy the equation

$$xr(1+A(z)) = \frac{q-1}{q}\sum_{i=1}^{r} iz^i. \tag{3}$$

Define the function

$$H_{q,r}(x) = x(1-\log_q z_0) + \frac{1}{r}\log_q(1+A(z_0)).$$

In the case $r=1$ we write $h_q(x)$ instead of $H_{q,1}(x)$, where

$$h_q(x) = -x\log_q \frac{x}{q-1} - (1-x)\log_q(1-x).$$

Let

$$\delta_{\text{crit}} = 1 - \frac{1}{r}\sum_{i=1}^{r} q^{-i} = 1 - \frac{1}{rq^r}\frac{q^r-1}{q-1}. \tag{4}$$

The asymptotic volume of the sphere in $\overrightarrow{H}$ is given in the next lemma.

Lemma 1.2. [34] *(a) For $0 < x < 1$, equation (3) has a unique positive root $z_0(x), z_0 \in [0, r]$.*
(b) Let $r \geq 1$ be fixed, $n \to \infty, d/n \to r\delta$, then

$$\lim_{n\to\infty}(nr)^{-1}\log_q\sum_{i=0}^{d} S_i = \begin{cases} H_{q,r}(\delta), & 0 \leq \delta \leq \delta_{\text{crit}}, \\ 1, & \delta_{\text{crit}} < \delta \leq 1. \end{cases} \tag{5}$$

2. Bounds on Ordered Codes and Arrays

In general, given the value of the distance or the strength, our goal is to construct as large codes and as small OOAs as possible. The latter will also account for small-size (t, m, s)-nets with bounded discrepancy. In this section we recall the known bounds on ordered codes and OOAs and derive a new bound on the size of codes.

2-A. **Existence bounds.**

A Gilbert-type bound on ordered codes was derived in [34].

Theorem 2.1. *There exists an (nr, M, d) code in the space $\overrightarrow{H}$ whose parameters satisfy*

$$M\sum_{i=0}^{d-1} S_i \geq q^{nr}.$$

If $\mathcal{Q}$ is a finite field, then there exists a linear code with the same parameters.

A bound that applies specifically to linear codes was proved in [8]. It is analogous to the Varshamov bound for the Hamming space.

Theorem 2.2. *Suppose that m and t satisfy the conditions*

$$\sum_{i=0}^{t-\tau} S_{i,n-1} < q^{m-(\tau-1)}, \quad \tau = 1, \dots, t-1.$$

Then there exists an $[nr, nr-m]$ linear code in $\overrightarrow{H}$ of distance $\geq t+1$, and a (t, n, r, q) linear OOA of dimension m.

2-B. **Nonexistence bounds.** While in general bounds on codes do not imply lower bounds on OOAs, there are two special cases when these two types of results are equivalent. First, if C is an $[nr, k, d]$ linear code over $\mathbb{F}_q^{nr}$ then the code $C' := \{\boldsymbol{y} \in \mathbb{F}_q^{nr} : \sum_{i=1}^{nr} x_i y_i = 0 \text{ for all } \boldsymbol{x} \in C\}$ is a $(d-1, n, r, q)$ linear OOA. Next, if an upper (lower) bound on codes (OOAs) is obtained by linear programming as explained in the next section then the same solution of the LP problem gives a lower (upper) bound on OOAs (codes).

We next mention some upper bounds on codes and OOAs.

2-B.1. *Singleton bound.* The parameters of any (nr, M, d) code satisfy

$$M \le q^{nr-d+1}.$$

2-B.2. *Plotkin bound.* A Plotkin bound on codes was established in [34]. Namely, the following result holds true.

Theorem 2.3. *Let $C \subset \overrightarrow{H}$ be a code of size M and distance $d > nr\delta_{\text{crit}}$. Then*

$$M \le \frac{d}{d - nr\delta_{\text{crit}}}.$$

A dual Plotkin bound on OOAs was proved by Martin and Visentin [26].

Theorem 2.4. [26] *Let C be a $[t, n, r, q]$ OOA. If $t > nr\delta_{\text{crit}} - 1$ then*

$$|C| \ge q^{nr}\Big(1 - \frac{nr\delta_{\text{crit}}}{t+1}\Big).$$

2-B.3. *Hamming-Rao bound.* According to the Hamming bound, the parameters of any $(nr, M, d = 2\tau + 1)$ code satisfy

$$M \le \frac{q^{rn}}{\sum_{i=0}^{\tau} S_i}.$$

A dual bound in this case is the Rao bound which for the NRT space was established by Martin and Stinson [25]: The size M of any $(t = 2\tau, n, r, q)$ OOA satisfies

$$M \ge \sum_{i=0}^{\tau} S_i.$$

2-B.4. *A Bassalygo-Elias bound on codes.* The next result is new.

Theorem 2.5. *Let C be an (nr, M, d) code. Then*

$$M \le q^{rn} dn \frac{1}{S_w(dn - 2wn + \frac{w^2}{r\delta_{crit}})}.$$

for any $w \le nr\delta_{\text{crit}}(1 - \sqrt{1 - d/(nr\delta_{\text{crit}})})$.

Proof : We will rely upon the next lemma.

Lemma 2.6. *Let $C \subset \overrightarrow{H}, |C| = M$ be a code all of whose vectors have weight w and are at least distance d apart. Then for $d \ge 2w - w^2/(nr\delta_{\text{crit}})$,*

$$M \le \frac{dn}{dn - 2wn + \frac{w^2}{r\delta_{crit}}}.$$

Proof : Let C^i be a projection of C on the ith block of coordinates. For a vector $\boldsymbol{z} \in \mathcal{Q}^r$ let $\boldsymbol{z}^h = (z_{r-h+1}, \dots, z_r)$ be its suffix of length h. Given $\boldsymbol{x} \in C$, we denote by $\boldsymbol{x}^i \in C^i$ its ith block and write $\boldsymbol{x}^{i,h}$ to refer to the h-suffix of $\boldsymbol{x}^i$. For $i = 1, \dots, n; h = 1, \dots, r; \boldsymbol{c} \in \mathcal{Q}^h$ let

$$\lambda_{i,\boldsymbol{c}}^h = |\{\boldsymbol{x}^i \in C^i : \ \boldsymbol{x}^{i,h} = \boldsymbol{c}\}|$$

be the number of vectors in the ith block whose h-suffix equals $\boldsymbol{c}$. We have

$$\begin{aligned} d_r(\boldsymbol{x}^i, \boldsymbol{y}^i) &= r - \sum_{h=1}^r \delta(\boldsymbol{x}^{i,h}, \boldsymbol{y}^{i,h}) \\ &= r - \sum_{h=1}^r \sum_{\boldsymbol{c} \in \mathcal{Q}^h} \delta(\boldsymbol{x}^{i,h}, \boldsymbol{c}) \delta(\boldsymbol{y}^{i,h}, \boldsymbol{c}). \end{aligned}$$

Compute the sum of all distances in the code as follows:

$$\begin{aligned} \sum_{\boldsymbol{x},\boldsymbol{y} \in C} d_r(\boldsymbol{x}, \boldsymbol{y}) &= nrM^2 - \sum_{i=1}^n \sum_{\boldsymbol{x}^i, \boldsymbol{y}^i \in C^i} \sum_{h=1}^r \sum_{\boldsymbol{c} \in \mathcal{Q}^h} \delta(\boldsymbol{x}^{i,h}, \boldsymbol{c}) \delta(\boldsymbol{y}^{i,h}, \boldsymbol{c}) \\ &= nrM^2 - \sum_{i=1}^n \sum_{h=1}^r \sum_{\boldsymbol{c} \in \mathcal{Q}^h} (\lambda_{i,\boldsymbol{c}}^h)^2. \end{aligned} \tag{6}$$

To bound above the right-hand side, we need to find the minimum of the quadratic form

$$F = \sum_{i=1}^n \sum_{h=1}^r \sum_{c \in \mathcal{Q}^h \backslash \{0\}} (\lambda_{i,c}^h)^2 + \sum_{i=1}^n \sum_{h=1}^r (\lambda_{i,0}^h)^2$$

under the constraints

$$\sum_{i=1}^n \sum_{h=1}^r \lambda_{i,0}^h = M(nr - w), \qquad \sum_{c \in \mathcal{Q}^h} \lambda_{i,c}^h = M \ (1 \le h \le r, \ 1 \le i \le n). \tag{7}$$

Critical points of F in the intersection of these hyperplanes, together with (7), satisfy the equations

$$\begin{matrix} 2\lambda_{i,c}^h + \beta_{i,h} = 0, & 1 \le i \le n; 1 \le h \le r; c \in \mathcal{Q}^h \backslash \{0\} \\ 2\lambda_{i,0}^h + \alpha + \beta_{i,h} = 0, & 1 \le i \le n; 1 \le h \le r \end{matrix} \qquad \alpha, \beta_{i,h} \in \mathbb{R}. \tag{8}$$

The system (7)-(8) has a unique solution for the variables $\lambda_{i,c}^h, \beta_{i,h}, \alpha$; in particular,

$$\begin{aligned} \lambda_{i,0}^h &= M\Big[\Big(\frac{1}{q^h} - 1\Big)\frac{w}{nr\delta_{\text{crit}}} + 1\Big], \quad h = 1, \dots, r, i = 1, \dots, n, \\ \lambda_{i,c}^h &= \frac{Mw}{q^h nr \delta_{\text{crit}}}, \qquad h = 1, \dots, r, i = 1, \dots, n, c \in \mathcal{Q}^h \backslash \{0\}. \end{aligned}$$

To verify that this critical point is in fact a minimum, observe that the form F is convex because its Hessian matrix is $2I$ and is positive definite (both globally and restricted to the intersection of the hyperplanes (7)). Substituting these values of the λs and taking account of the fact that $\sum_h q^{-h} = r(1 - \delta_{\text{crit}})$, we get

$$\begin{aligned} F &\ge \sum_{i=1}^n \sum_{h=1}^r \sum_{c \ne 0} \Big(\frac{Mw}{q^h nr \delta_{\text{crit}}}\Big)^2 + \sum_i \sum_h M^2 \Big[\Big(\frac{1}{q^h} - 1\Big)\frac{w}{nr\delta_{\text{crit}}} + 1\Big]^2 \\ &= M^2 n\Big(\frac{w^2}{n^2 r \delta_{\text{crit}}} - \frac{2w}{n} + r\Big). \end{aligned}$$

Then from (6) we obtain

$$dM(M-1) \le \sum_{\boldsymbol{x},\boldsymbol{y}\in C} d_r(\boldsymbol{x},\boldsymbol{y}) \le \frac{M^2}{n}\Big(2wn - \frac{w^2}{r\delta_{\text{crit}}}\Big)$$

which gives the result. ∎

The proof of the theorem is completed as follows. Let $\mathcal{S}_w \subset \mathcal{Q}^{r,n}$ be a sphere of radius w around zero. Clearly,

$$|C||\mathcal{S}_w| = \sum_{x\in\overrightarrow{H}} |(C-x)\cap \mathcal{S}_w| \le q^{nr}A_q(nr,d,w),$$

where $A_q(nr,d,w)$ is the maximum size of a distance-d code in $\mathcal{S}_w$. With the previous lemma, this finishes the proof. ∎

Remarks. 1. This theorem implies a lower bound on the size M of a linear OOA $(t-1,n,r,q)$: for any $w \le nr\delta_{\text{crit}}(1-\sqrt{1-t/(nr\delta_{\text{crit}})})$,

$$M \ge \frac{1}{tn} S_w\Big(tn - 2wn + \frac{w^2}{r\delta_{\text{crit}}}\Big) \tag{9}$$

and in particular, a lower bound on linear $(m-r,m,n)$-nets, $m = \log_q M$.

2. Caution should be exercised in dealing with codes of a constant weight in the NRT space, i.e., codes on the sphere $\mathcal{S}_w$ in $\overrightarrow{H}$. Indeed, the sphere $\mathcal{S}_w$ together with the metric d_r is not homogeneous: in particular, the number of points in $\mathcal{S}_w$ located at a given distance from a point $x \in \mathcal{S}_w$ depends on x. However, this does not cause problems in the previous theorem.

3. The argument used in the proof of Lemma 2.6 can be also used to give a proof of the Plotkin bound, Theorem 2.3, that is simpler than the ones known in the literature. Indeed, let $C \subset \overrightarrow{H}$ be a distance-d code. Consider again expression (6) and note that this time there is no restriction on the weight of the codewords. Using the Cauchy-Schwarz inequality and the fact that $\sum_{\boldsymbol{c}\in\mathbb{F}_q^h} \lambda_{i,\boldsymbol{c}}^h = M$, we obtain

$$M(M-1)d \le nrM^2 - \sum_{i=1}^n\sum_{h=1}^r \frac{M^2}{q^h} = nrM^2\delta_{\text{crit}}.$$

Solving for M concludes the proof.

2-B.5. *Asymptotics.* In this section we assume that $n\to\infty$ and r is a constant. For a code of size M let $R = \log_q M/nr$ be the code *rate*. Given a sequence of (rn_i, M_i, d_i) codes we will say that its *asymptotic rate* is R and the asymptotic relative distance is δ if

$$\lim_{i\to\infty}\frac{1}{rn_i}\log_q M_i = R, \quad \lim_{i\to\infty}\frac{d_i}{rn_i} = \delta.$$

The Plotkin bound implies that the asymptotic rate and distance of any sequence of codes satisfy

$$\begin{aligned} &R \le 1 - \frac{\delta}{\delta_{\text{crit}}}, && 0 \le \delta \le \delta_{\text{crit}},\\ &R = 0, && \delta \ge \delta_{\text{crit}}. \end{aligned}$$

To state the "sphere packing" or "volume" bounds on ordered codes we rely upon Lemma 1.2. Namely [34], there exists a sequence of $[rn_i, k_i, d_i]$ linear codes $C_i, i = 1, 2, \dots$, such that $n_i \to \infty$, $k_i/(rn_i) \to R$, $d_i/(rn_i) \to \delta$ and

$$R \geq 1 - H_{q,r}(\delta), \quad 0 \leq \delta \leq \delta_{\text{crit}} \qquad \text{(Gilbert-Varshamov bound)}.$$

On the other hand, for any such sequence of codes,

$$R + H_{q,r}(\delta/2) \leq 1 \qquad \text{(Hamming bound)}.$$

The asymptotic version of Theorem 2.5 is as follows:

Theorem 2.7. (Asymptotic Bassalygo-Elias bound). *For* $0 \leq \delta \leq \delta_{\text{crit}}$ *the asymptotic rate and distance of any sequence of codes satisfy*

$$R \leq 1 - H_{q,r}\Big(\delta_{\text{crit}}(1 - \sqrt{1 - \delta/\delta_{\text{crit}}})\Big). \tag{10}$$

This bound is better than the Hamming bound for all $\delta \in (0, \delta_{\text{crit}}]$. It is also often better than the Plotkin bound. For instance, for $q = 2, r = 2$ the bound (10) is better than the Plotkin bound for all $\delta \in (0, \delta_{\text{crit}})$. For larger q, r the improvement is attained only for low values of δ since the right-hand side of (10) becomes $\cap$-convex close to δ_{crit}. For instance, for $q = 3, r = 4$ this range is $(0, 0.54)$, etc.

2-B.6. *Asymptotic bounds for digital* (t, m, s)*-nets.* A (t, m, s)-net is called digital if the OOA that corresponds to it forms a linear subspace of $\mathbb{F}_q^{nr}$. Therefore, bounds on linear OOAs apply to the special case of digital (t, m, s)-nets. However, studying asymptotics for this case requires a different normalization since the strength $m - t$ of the OOA that corresponds to the net equals r, and both approach infinity independently of s. Therefore, let $R = m/s$ denote the rate and $\delta = (m-t)/s$ denote the relative strength of the OOA that corresponds to the net. To state the bounds, we need to compute the asymptotic behavior of the volume of the sphere, which is different from (5). The next result is due to Bierbrauer and Schmid [9].

Theorem 2.8. *There exist families of digital* (t, m, s)*-nets with* $s, (m - t) \to \infty$ *for which* (R, δ) *satisfy the bound* $R \leq \Psi(\delta)$, *where*

$$\Psi(\delta) = \delta - 1 + \log_q\left(\frac{q - 1 + \alpha}{\alpha}\right) - \delta \log_q(1 - \alpha),$$

and α *is defined by* $\delta\alpha(q - 1 + \alpha) = (q - 1)(1 - \alpha)$.

On the other hand, by the Rao bound, any family of (t, m, s)-nets satisfies $R \geq \Psi(\delta/2)$. Observe that Theorem 2.5 in this case gives the same result as the Rao bound because the increase of the packing radius in (9) over $\delta/2$ vanishes asymptotically. Indeed, taking $\omega = w/n$ and replacing t with $m - t$, we obtain from (9)

$$M \geq \frac{1}{\delta}(\delta - 2\omega + o(1))S_{\omega n}.$$

The tightest bound is obtained if we take $\omega = \delta/2$ in this inequality.

Remark: We note that in the case that both $n \to \infty$ and $r \to \infty$ while $\delta = d/nr$ tends to a constant bounded away from 0 and 1, the lower and upper bounds on codes coincide [34] (the Gilbert-Varshamov bound converges to the Singleton bound).

3. ASSOCIATION SCHEMES, AND THE ORDERED HAMMING SCHEME

The coding-theoretic notion of duality prompted a study of the association scheme that describes the combinatorics of the NRT space. We briefly recall some elements of Delsarte's theory of association schemes [13]. A symmetric association scheme with D classes is a finite set $X, |X| = N$, equipped with a set $\mathcal{R} = \{R_0, R_1, \dots, R_D\}$ of symmetric binary relations on $X \times X$ such that

(i) $R_0 = \{(x, x)\},\ R_i \cap R_j = \emptyset,\ \cup_{i=0}^{D} R_i = X \times X$;

(ii) For each $0 \le i, j, k \le D$ the number

$$p_{i,j}^k = |\{(x, y) \in R_i, (x, z) \in R_j \text{ given that } (y, z) \in R_k\}|$$

depends only on (i, j, k). Moreover, $p_{i,j}^k = p_{j,i}^k$.

The parameters $p_{i,j}^k$ are called the intersection numbers of the scheme $\mathcal{A} = (X, \mathcal{R})$. The numbers $v_i = p_{i,i}^0$ are called the valencies of $\mathcal{A}$. Let A_i be the adjacency matrix of the relation $R_i, i = 0, \dots, D$. It is clear that

$$A_0 = I,\ \sum_{i=0}^{D} A_i = J \quad \text{(all-one matrix)},$$

and for all $0 \le i, j \le D$ the product $A_i A_j$ is contained in the linear span of $\{A_0, A_1, \dots, A_D\}$. The matrices A_i form a commutative algebra over $\mathbb{C}$ with respect to matrix multiplication, called the Bose-Mesner algebra.

It is clear that the Bose-Mesner algebra is also closed under the Hadamard (element-wise) multiplication $\circ$, viz. $A_i \circ A_j = \delta_{i,j} A_j$. With respect to $\circ$, this algebra has a basis of primitive idempotents $\{E_0, E_1, \dots, E_D\}$ that satisfy

$$E_0 = \frac{1}{N} J, \quad E_i \circ E_j = \frac{1}{N} \sum_{k=0}^{D} q_{i,j}^k E_k,\ 0 \le i, j \le D.$$

The numbers $q_{i,j}^k$ are nonnegative. They are called the Krein parameters of the association scheme. The quantities $\mu_i = q_{i,i}^0$ are called multiplicities of the scheme $\mathcal{A}$. The matrices P and Q defined by

$$A_i = \sum_{j=0}^{D} P_{ji} E_j, \quad 0 \le i \le D,$$

and

$$E_j = \frac{1}{N} \sum_{i=0}^{D} Q_{ij} A_i, \quad 0 \le j \le D,$$

are called the *first* and *second eigenvalues* of $\mathcal{A}$, respectively. The eigenvalue matrices satisfy $PQ = NI$. Further, for $0 \le i, j \le D$ the eigenvalues satisfy

$$\mu_i P_{ij} = v_j Q_{ji}, \tag{11}$$

$$\sum_{k=0}^{D} \mu_k P_{ki} P_{kj} = N v_i \delta_{ij}, \tag{12}$$

$$P_{ij} P_{ik} = \sum_{l=0}^{D} p_{j,k}^l P_{il}, \quad 0 \le i \le D. \tag{13}$$

Two D-class association schemes are called Delsarte duals of each other if the adjacency matrices A_i, the first eigenvalues P, and the intersection numbers $p_{i,j}^k$ of one scheme are, respectively, the idempotents E_i, the second eigenvalues Q and the Krein numbers $q_{i,j}^k$ of the other. The duality also exchanges the role of the matrix and Hadamard multiplication. A scheme is called *self-dual* if it equals its dual. For instance, the Hamming scheme $H_n = (X = \mathcal{Q}^n, R_i = \{(x,y) \in X, d_H(x,y) = i\}, i = 0, \dots, n)$ is self-dual. One of the manifestations of self-duality in this case, obvious from the definition, is the MacWilliams theorem that relates the weight distribution of an additive code to that of its dual. A scheme is called *formally self-dual* [11] if there exists some ordering of primitive idempotents under which $P = Q$. In a formally self-dual scheme $v_i = \mu_i$ and $p_{i,j}^k = q_{i,j}^k$. Following Delsarte [13, p. 17] a scheme $(X^n, \mathcal{R})$ is called an *extension* of an r-class scheme $\mathcal{K} = (X, \mathcal{D} = (D_0, D_1, \dots, D_r))$ if its vertex set is the n-fold Cartesian product of X and the relations $R_e, e \in \Delta_{r,n}$ are given by

$$R_e = \{((x_{11}, \dots, x_{1n}), (x_{21}, \dots, x_{2n})) : \\ |\{j : (x_{1j}, x_{2j}) \in D_i\}| = e_i,\ i = 0, 1, \dots, r\}.$$

Apart from [13] we refer to [5, 11, 18] for the proofs of these results and more information on association schemes.

The association scheme for the NRT space was constructed and studied by Martin and Stinson [24]. Define an r-class "kernel scheme" $\mathcal{K}(\mathcal{Q}^{r,1}, \mathcal{D} = (D_0, D_1, \dots, D_r))$ with the relations

$$D_i = \{(\boldsymbol{x}_1, \boldsymbol{x}_2) \in \mathcal{Q}^{r,1} \times \mathcal{Q}^{r,1} : d_r(\boldsymbol{x}_1, \boldsymbol{x}_2) = i\}, \quad i = 0, 1, \dots, r.$$

Theorem 3.1. [24] *The space $X = \mathcal{Q}^{r,n}$ together with the relations*

$$R_e = \{(\boldsymbol{x}, \boldsymbol{y}) \in X \times X : \boldsymbol{x} \sim_e \boldsymbol{y}\} \quad (e \in \Delta_{r,n})$$

forms a formally self-dual association scheme $\overrightarrow{\mathcal{H}}$, called the r-Hamming scheme. It can be constructed as an n-fold Delsarte extension of $\mathcal{K}$.

The dual scheme of $\overrightarrow{\mathcal{H}}$ is $\overleftarrow{\mathcal{H}}$ whose point set is $X = \mathcal{Q}^{r,n}$ and the set of relations is given by

$$R_e = \{(\boldsymbol{x}, \boldsymbol{y}) \in X \times X : \overline{\text{shape}}(\boldsymbol{x} - \boldsymbol{y}) = e\} \quad (e \in \Delta_{r,n}).$$

4. Multivariate Krawtchouk Polynomials

In the conventional case of $r = 1$, eigenvalues of the Hamming scheme are given by the Krawtchouk polynomials

$$k_i(n, x) = \sum_{l=0}^{i} (-1)^l (q-1)^{k-l} \binom{x}{\ell} \binom{n-x}{k-\ell} \tag{14}$$

which form a family of polynomials of one discrete variable orthogonal on the set $\{0, 1, \dots, n\}$ with weight $\alpha(i) = \binom{n}{i}(q-1)^i q^{-n}$, i.e., the binomial probability distribution. Here we are interested in their generalization for the r-Hamming scheme.

Observe that the valencies $v_e = p_{e,e}^0$ of the scheme are given by (1). By self-duality and (12), the eigenvalues are orthogonal on the space of partitions $\Delta_{r,n}$ with weight v_e. Below it will be convenient to normalize the weight. Let $V = V_{r,n}$ be the space of real polynomials of r discrete variables $x = (x_1, x_2, \dots, x_r)$ defined on $\Delta_{r,n}$. Let us define a bilinear form acting on the space V by

$$\langle u_1, u_2 \rangle = \sum_{e \in \Delta_{r,n}} u_1(e) u_2(e) w(e), \tag{15}$$

where $w(e) = q^{-nr} v_e$. Letting $p_i = q^{i-r-1}(q-1), i = 1, \dots, r$; $p_0 = q^{-r}$, we observe that

$$w(e) = n! \prod_{i=0}^{r} \frac{p_i^{e_i}}{e_i!}$$

forms a multinomial probability distribution on $\Delta_{r,n}$. Therefore, r-variate polynomials orthogonal with respect to this weight form a particular case of multivariate Krawtchouk polynomials.

For a partition $f \in \Delta_{r,n}$ denote by

$$K_f(x) = K_{f_1,\dots,f_r}(x_1, \dots, x_r)$$

the Krawtchouk polynomial that corresponds to it. Let $\kappa = |f|$ be the degree of K_f.

Our goal in this section is to derive properties of the polynomials K_f. In their large part, these properties are obtained by specializing to the current case general relations of the previous section. However, some work is needed to transform them to a concrete form which will be used in later calculations.

The following relations are useful below.

Lemma 4.1.

$$\langle x_i, 1\rangle = n(q-1)q^{i-r-1}, \qquad i = 1, \dots, r \tag{16}$$

$$\langle x_i, x_j\rangle = n(n-1)(q-1)^2 q^{i+j-2r-2}, \qquad 1 \le i \ne j \le r \tag{17}$$

$$\langle x_i, x_i\rangle = n(q-1)q^{i-r-1}(1 + (n-1)(q-1)q^{i-r-1}), \qquad i = 1, \dots, r. \tag{18}$$

Proof : To prove (16), compute

$$\langle x_i, 1\rangle = q^{-nr} \sum_e \left\{ e_i \binom{n}{e_0, e_1, \dots, e_r} \prod_{j=1}^{r} ((q-1)q^{j-1})^{e_j} \right\}$$

$$= nq^{-nr} \sum_e \binom{n-1}{e_0, e_1, \dots, e_i - 1, \dots, e_r} \prod_{j=1}^{r} ((q-1)q^{j-1})^{e_j}.$$

The sum on e on the last line equals $(q-1)q^{i-1+(n-1)r}$ which finishes the proof. The remaining two identities are proved in a similar way. ∎

4-A. **Properties of the polynomials K_e.**

(i) $K_e(x)$ is a polynomial in the variables $x_1, \dots, x_r$ of degree $\kappa = |e|$. There are $\binom{\kappa+r-1}{r-1}$ different polynomials of the same degree, each corresponding to a partition of κ.

(ii) (*Orthogonality*) Equation (12) is rewritten as

$$\langle K_f, K_g\rangle = v_f \delta_{f,g}, \quad \|K_f\| = \sqrt{v_f}. \tag{19}$$

In particular, let $F_i = (0^{i-1}10^{r-i-1}), i = 1, \dots, r$ be a partition with one part. We have

$$\|K_{F_i}\|^2 = \langle K_{F_i}, K_{F_i}\rangle = n(q-1)q^{i-1}, \quad i = 1, \dots, r. \tag{20}$$

Indeed, equality (19) is simply (12) specialized to the case at hand and (20) is obtained from (1).

(iii) (*Linear polynomials*) For $i = 1, \dots, r$,

$$K_{F_i}(x) = q^{i-1}(q-1)(n - x_r - \dots - x_{r-i+2}) - q^i x_{r-i+1}. \tag{21}$$

Proof: This is shown by orthogonalizing the set of linear polynomials $(1, x_1, x_2, \dots, x_r)$. We take $K_{0,\cdots,0} = 1$. Use Lemma 4.1 to compute

$$K_{F_1}(x) = c_1(x_r - \langle x_r, 1\rangle) = c_1(x_r - n(q-1)/q)$$

for some constant c_1. To find c_1, use (20):

$$n(q-1) = c_1^2 \|x_r - \frac{n(q-1)}{q}\|^2 = c_1^2 n(q-1)q^{-2}.$$

Hence $c_1 = \pm q$. We take $K_{F_1}(x) = n(q-1) - qx_r$ choosing $c_1 = -q$ so that $K_{F_1}(0) > 0$.

Next let us perform the induction step to compute $K_{F_{i+1}}(x)$:

$$K_{F_{i+1}}(x) = c_{i+1}\Big(x_{r-i} - \sum_{j=0}^{i} \|K_{F_j}\|^{-2}\langle x_{r-i}, K_{F_j}\rangle K_{F_j}(x)\Big), \tag{22}$$

where the polynomials $K_{F_j}, j = 0, \dots, i,$ have the form (21) by the induction hypothesis. Straightforward calculations using (16)-(18) show that

$$K_{F_{i+1}}(x) = c_{i+1}(x_{r-i} - ((q-1)/q)(n - x_r - \cdots - x_{r-i+1})).$$

Again using (20), we find that $c_{i+1} = \pm q^{i+1}$; as above, we will choose the minus. ∎

(iv) The next property is a special case of (11).

$$v_e K_f(e) = v_f K_e(f) \quad (e, f \in \Delta_{r,n}).$$

In particular,

$$K_f(0) = v_f. \tag{23}$$

(v) For any $f, g \in \Delta_{r,n}$

$$K_f(e)K_g(e) = \sum_{h\in\Delta_{r,n}} p_{f,g}^h K_h(e) \tag{24}$$

where the linearization coefficients $p_{f,g}^h = |\{\boldsymbol{z} \in \mathcal{Q}^{r,n} : \boldsymbol{z} \sim_f \boldsymbol{x}, \boldsymbol{z} \sim_g \boldsymbol{y}; \boldsymbol{x} \sim_h \boldsymbol{y}\}|$ are the intersection numbers of the scheme. In particular, $p_{f,g}^h \ge 0$. This is a special case of property (13).

(vi) (*Three-term relation*) Let $\mathbb{K}_\kappa$ be a column vector of the polynomials K_f ordered lexicographically with respect to all f that satisfy $|f| = \kappa$. The three-term relation is obtained by expanding a product $P(e)\mathbb{K}_\kappa(e)$ in the basis $\{K_f\}$, where $P(e)$ is a first-degree polynomial. By orthogonality, the only nonzero terms in this expansion will be polynomials of degrees $\kappa+1, \kappa, \kappa-1$ [15, p. 75].

We will establish an explicit form of the three-term relation for $P(e) = \delta_{\text{crit}} rn - |e|'$. We have

$$P(e)\mathbb{K}_\kappa(e) = a_\kappa \mathbb{K}_{\kappa+1}(e) + b_\kappa \mathbb{K}_\kappa(e) + c_\kappa \mathbb{K}_{\kappa-1}(e), \tag{25}$$

where $a_\kappa, b_\kappa, c_\kappa$ are matrices of order $\binom{\kappa+r-1}{r-1} \times \binom{\kappa+s+r-1}{r-1}$ and $s = 1, 0, -1$, respectively. The nonzero elements of these matrices have the following form:

$$\begin{aligned} a_\kappa[f,h] &= L_i(f_i+1) && \text{if } h = (f_1, \dots, f_i+1, \dots, f_r), \\ c_\kappa[f,h] &= L_i(n-\kappa+1)q^{i-1}(q-1) && \text{if } h = (f_1, \dots, f_i-1, \dots, f_r), \end{aligned}$$

(26)

$$b_\kappa[f,h]=\begin{cases} L_i f_i q^{i-1}(q-2) & \text{if } h=f,\\ L_i(f_k+1)q^{i-1}(q-1) & \text{if } h=(f_1,\dots,f_k+1,\dots,f_i-1,\dots,f_r),\\ & \quad 1\le k<i,\\ L_i(f_i+1)q^{k-1}(q-1) & \text{if } h=(f_1,\dots,f_k-1,\dots,f_i+1,\dots,f_r),\\ & \quad 1\le k<i,\end{cases}$$

where $L_i=\frac{q^{r-i+1}-1}{q^r(q-1)}$.

Proof: According to Property (v), the coefficients of the expansion of the product $K_{F_i}(e)K_f(e)$ into the basis $\{K_h\}$ are given by the intersection numbers of the scheme:

$$K_{F_i}(e)K_f(e)=\sum_h p^h_{F_i,f}K_h(e). \tag{27}$$

Because the ordered metric is translation-invariant, we can assume that $\boldsymbol{y}=0$, so $p^h_{F_i,f}$ is the number of vectors $\boldsymbol{z}\sim_f 0$ that satisfy $\boldsymbol{z}\sim_{F_i}\boldsymbol{x}$ for a fixed vector $\boldsymbol{x}\sim_h 0$. In other words,

$$\boldsymbol{z}-\boldsymbol{x}=(0^r,\dots,0^r,(u_1,\dots,u_{i-1},u_i,0,\dots,0),0^r,\dots,0^r) \tag{28}$$

where the nonzero block is located in any of the n possible blocks, $u_j\in\mathbb{F}_q, 1\le j< i, u_i\neq 0$.

The numbers $p^h_{F_i,f}$ are nonzero only in the three following cases.

(1) $|h|=|f|+1$. By the above we have that $h_j=f_j$ for $j\neq i$ and $h_i=f_i+1$. Hence z can be chosen so that its f_i blocks of weight i annihilate the corresponding blocks of x, leaving one such block in any of the $h_i=f_i+1$ locations. Thus,

$$p^h_{F_i,f}=\begin{cases} f_i+1, & h=(f_1,\dots,f_i+1,\dots,f_r)\\ 0 & \text{otherwise.}\end{cases}$$

(2) $|h|=|f|$. The following numbers are easily verified by (28):

$$p^h_{F_i,f}=\begin{cases} f_i(q-2)q^{i-1}, & h=f,\\ (f_k+1)(q-1)q^{i-1}, & h=(f_1,\dots,f_k+1,\dots,f_i-1,\dots,f_r), 1\le k<i,\\ (f_i+1)(q-1)q^{k-1}, & h=(f_1,\dots,f_k-1,\dots,f_i+1,\dots,f_r), 1\le k<i,\\ 0 & \text{otherwise.}\end{cases}$$

Other than these three cases, no other possibilities for h arise.

(3) $|h|=|f|-1$. Now we should add to x one block of weight i in any of the $n-|f|+1$ all-zero blocks. Thus we obtain

$$p^h_{F_i,f}=(n-|f|+1)q^{i-1}(q-1)\quad h=(f_1,\dots,f_i-1,\dots,f_r)$$

and $p^h_{F_i,f}=0$ for all other h.

To prove (25) we now need to represent $P(e)$ as a linear combination of the K_{F_i}s. Using (21) we find that

$$|e|'=\sum_i ie_i=\delta_{\text{crit}}rn-\sum_{i=1}^r L_iK_{F_i}(e),$$

hence

$$P(e)=\sum_{i=1}^r L_iK_{F_i}(e). \tag{29}$$

The proof is now concluded by using (27) together with the intersection numbers computed above. ∎

Along with the polynomials K_e below we use their normalized version $\widetilde{K}_e = K_e/\sqrt{v_e}$. The polynomials $(\widetilde{K}_e, e \in \Delta_{r,n})$ form an orthonormal basis of V.

Denote by $A_\kappa, B_\kappa, C_\kappa$ the coefficient matrices of the normalized form of relation (25). The new matrix elements are given by

$$
\begin{aligned}
&A_\kappa[f,h] = L_i\sqrt{(f_i+1)(n-\kappa)q^{i-1}(q-1)} \qquad \text{if } h=(f_1,\dots,f_i+1,\dots,f_r),\\
&C_\kappa[f,h] = L_i\sqrt{(n-\kappa+1)f_iq^{i-1}(q-1)} \qquad \text{if } h=(f_1,\dots,f_i-1,\dots,f_r),
\end{aligned}
\tag{30}
$$

$$
B_\kappa[f,h] = \begin{cases} L_if_iq^{i-1}(q-2) & \text{if } h=f,\\[1ex] L_i\dfrac{q-1}{q}\sqrt{(f_k+1)f_iq^{k+i}} & \text{if } h=(f_1,\dots,f_k+1,\dots,f_i-1,\dots,f_r),\\ & \quad 1\le k<i,\\ L_i\dfrac{q-1}{q}\sqrt{f_k(f_i+1)q^{k+i}} & \text{if } h=(f_1,\dots,f_k-1,\dots,f_i+1,\dots,f_r),\\ & \quad 1\le k<i. \end{cases}
$$

Let $V_\kappa \subset V$ be the set of polynomials of total degree $\le \kappa$. Let E_κ be the orthogonal projection of V on V_κ. Define the operator

$$
\begin{aligned}
S_\kappa : &V_\kappa \to V_\kappa\\
&f \mapsto E_\kappa(Pf).
\end{aligned}
$$

Its matrix in the orthonormal basis has the form

$$
\widetilde{\mathbf{S}}_\kappa = \begin{bmatrix} B_0 & A_0 & 0 & \dots & 0\\ C_1 & B_1 & A_1 & \dots & 0\\ 0 & C_2 & B_2 & \dots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \dots & C_\kappa & B_\kappa \end{bmatrix}
$$

where the B_is are symmetric and $C_i = A_{i-1}^T, i=1,\dots,\kappa$. On account of property (v) and (29), the matrix elements of $\widetilde{\mathbf{S}}_\kappa$ are nonnegative.

The matrix of S_κ in the basis $\{K_f\}$ has the property

$$
v_h\mathbf{S}_\kappa[f,h] = v_f\mathbf{S}_\kappa[h,f] \quad (f,h\in\Delta_{r,n}). \tag{31}
$$

(vii) (*Explicit expression*)

$$
K_f(x) = q^{|f|'-|f|}\prod_{i=1}^r k_{f_i}(n_i, x_{r-i+1}), \tag{32}
$$

where k_{f_i} is a univariate Krawtchouk polynomial (14), $n_i = \sum_{j=0}^{r-i+1} x_j - \sum_{j=i+1}^r f_j$, and $f,x\in\Delta_{r,n}$. This form of the polynomial $K_f(x)$ was obtained in [10] (various other forms were found in [24, 14]). We remark that (32) can be proved by performing the Gram-Schmidt procedure (22) for monomials of higher degrees. It is known that the resulting system of polynomials is unique up to a constant factor once the polynomials of degrees 0 and 1 together with the three-term relation (25) have been fixed, see [15, Theorem 3.4.9].

(viii) The matrix elements of the eigenvalue matrices of the association scheme $\overrightarrow{H}$ are given by $P_{fe} = Q_{fe} = K_f(e)$. This follows from the previous property and (12) because

the polynomials $\{K_f\}$ form a unique orthogonal family on $\Delta_{r,n}$ with respect to the weight $w(e)$.

(ix) (*Fourier transform representation*) Let ω be a qth degree primitive root of unity, $e, f \in \Delta_{r,n}$. Then

$$K_f(e) = \sum_{\boldsymbol{z}:\boldsymbol{z}\sim_f 0} \omega^{\boldsymbol{x}\cdot\boldsymbol{z}} \tag{33}$$

where $\overline{\text{shape}}(\boldsymbol{x}) = e$. In [10] this relation is taken as a definition of the polynomials K_f. Under our approach, it follows from the well-known Fourier transform representation of the Krawtchouk polynomials $k_i(n, x)$ in the case $r = 1$ and Theorem 3.1.

(x) (*Christoffel-Darboux*). Let $L \subset \Delta_{r,n}$ and define

$$U_L(a, e) \triangleq \sum_{f\in L} v_f^{-1} K_f(a) K_f(e) \quad (a, e \in \Delta_{r,n}).$$

Let $\mathbf{S}$ be the matrix of the operator $S : V_n \to V_{n+1}$ given by $f \mapsto Pf$, written in the basis $\{K_f\}$. The action of $P(e)$ on U_L is described as follows:

$$\begin{aligned}(P(e) - P(a))U_L(a, e) &= \sum_{f\in L} v_f^{-1} \sum_{h\in\Delta_{r,n}} \mathbf{S}[f, h](K_h(e)K_f(a) - K_h(a)K_f(e))\\ &= \sum_{f\in L} v_f^{-1} \sum_{h\in\Delta_{r,n}\setminus L} \mathbf{S}[f, h](K_h(e)K_f(a) - K_h(a)K_f(e)),\end{aligned}$$

the last equality justified by (31) as follows:

$$\begin{aligned}&\sum_{f,h\in L} v_f^{-1}\mathbf{S}[f, h](K_h(e)K_f(a) - K_h(a)K_f(e))\\ =&\sum_{f,h} \mathbf{S}[f, h]\sqrt{\frac{v_h}{v_f}}(\widetilde{K}_h(e)\widetilde{K}_f(a) - \widetilde{K}_f(e)\widetilde{K}_h(a))\\ =&0.\end{aligned}$$

A particular case of the above is obtained when $L = \{f : |f| \le \kappa\}$. The kernel U_L, denoted in this case by U_κ, equals $U_\kappa = \sum_{s=0}^{\kappa} \widetilde{\mathbb{K}}_s(e)^T \widetilde{\mathbb{K}}_s(a)$, and we obtain

$$\begin{aligned}(P(e) - P(a))U_\kappa(a, e) &= \widetilde{\mathbb{K}}_{\kappa+1}(e)^T A_\kappa^T \widetilde{\mathbb{K}}_\kappa(a) - \widetilde{\mathbb{K}}_\kappa(e)^T A_\kappa \widetilde{\mathbb{K}}_{\kappa+1}(a)\\ &= \sum_{f:|f|=\kappa} Q_f(e)\widetilde{K}_f(a) - \widetilde{K}_f(e)Q_f(a),\end{aligned} \tag{34}$$

where $Q_f(e) = \sum_{|h|=\kappa+1} \widetilde{K}_h(e)A_\kappa[f, h]$. This relation is called the Christoffel-Darboux formula.

(xi) The generating function of the polynomials K_f is given by

$$\sum_f K_f(e)z^f = \Big(1+(q-1)\sum_{i=1}^{r} q^{i-1}z_i\Big)^{n-|e|} \prod_{j=1}^{r} \Big(1+(q-1)\sum_{k=1}^{j-1} q^{k-1}z_k - q^{j-1}z_j\Big)^{e_{r-j+1}}.$$

In particular,

$$\sum_{f\in\Delta_{r,n}} K_f(e) = q^{rn}\delta_{e,0}.$$

Remarks: 1. The polynomials K_e were considered in [24, 14, 10]. However none of these papers constructed them from their definition as eigenvalues of the r-Hamming scheme

(to be more precise, Martin and Stinson [24] mention this approach but pursue the path suggested in Theorem 3.1 which makes explicit calculations difficult). Under the approach taken above, many properties of the polynomials K_e follow as special cases of the general combinatorial results of the previous section.

2. Other generalizations of univariate Krawtchouk polynomials were considered earlier in [37, 33]. These papers study biorthogonal polynomials for the weight given by the multinomial probability distribution, resulting in polynomial families different from the one considered above.

3. Property (xi) implies a MacWilliams theorem for NRT codes. It was previously proved in [24, 14] using different means.

Theorem 4.2. (MacWilliams theorem in the NRT space). *Let $C \subset \overrightarrow{H}$ and $C^\perp \subset \overleftarrow{H}$ be two linear codes that satisfy $\sum_{i=1}^{nr} x_i y_i = 0$ for every $\boldsymbol{x} \in C, \boldsymbol{y} \in C^\perp$. Let $A(z_0, z) = \sum_e A_e \prod_{i=0}^r z_i^{e_i}$ be the weight enumerator of C and let $A^\perp(z_0, z)$ be the same for $C^\perp$. Then*

$$A^\perp(z_0, z_1, \dots, z_r) = \frac{1}{|C|} A(u_0, u_1, \dots, u_r)$$

where

$$u_0 = z_0 + (q-1)\sum_{i=1}^r q^{i-1} z_i, \quad u_{r-j+1} = z_0 + (q-1)\sum_{k=1}^{j-1} q^{k-1} z_k - q^{j-1} z_j, 1 \le j \le r.$$

5. A Linear Programming Bound on Codes and OOAs

In this section we prove one of our main results, an LP bound on the rate of codes. Let $\mathsf{K} = (K_f(e))_{f,e\in\Delta_{r,n}}$ be the eigenvalue matrix of the r-Hamming scheme, where for definiteness we are assuming the lexicographic order on the partitions. Let $\mathsf{A} = (A_e), e \in \Delta_{r,n}$, be a vector of nonnegative real variables, with the same ordering. Define two linear programs,

$$\begin{array}{ll}
\text{(I)}: \ \sum_{e\neq 0} A_e \to \max & \\
\quad \text{subject to} & \\
\quad (\mathsf{AK})_e \ge 0, & \text{for all } e \\
\quad A_e = 0 & |e|' \le d-1,
\end{array}
\qquad
\begin{array}{ll}
\text{(II)}: \ \sum_{e\neq 0} A_e \to \min & \\
\quad \text{subject to} & \\
\quad (\mathsf{AK})_e = 0, & |e|' \le t \\
\quad (\mathsf{AK})_e \ge 0, & |e|' > t \\
\quad A_e \ge 0, &
\end{array}$$

and let LP(I) and LP(II) be their solutions. Let $C(nr, M, d)$ be a code and $C'(t, n, r, q)$ be an OOA of size M'. Then it follows from Delsarte's work [13] that

$$M \le LP(\text{I}), \quad M' \ge LP(\text{II}).$$

Replacing the LP problems by their duals, we obtain the following theorem.

Theorem 5.1. *Let $F(x) = F_0 + \sum_{e\neq 0} F_e K_e(x)$ be a polynomial that satisfies*

$$F_0 > 0, \quad F_e \ge 0 \ \ (e \ne 0); \quad F(e) \le 0 \ \ \textit{for all } e \textit{ such that } |e|' \ge d. \tag{35}$$

Then any (nr, M, d) code satisfies

$$M \le F(0)/F_0. \tag{36}$$

Any OOA of strength $t = d-1$ and size M' satisfies

$$M' \ge q^{nr} F_0 / F(0). \tag{37}$$

This result is essentially due to P. Delsarte. However, for the NRT space it was first stated by Martin [24, 22] and later rederived by Bierbrauer [10]. The fact that the same polynomial gives a bound both on codes and orthogonal arrays is an easy consequence of Delsarte's theory, first mentioned in Levenshtein's work [21].

5-A. **The bound.** In this section we use Theorem 5.1 to derive a bound on ordered codes and arrays. Its proof uses a "spectral method" first employed in [4] for the Grassmannian space and later used in [6] to prove classical asymptotic bounds of coding theory. The gist of the method can be explained as follows. The polynomial $F(e)$ is sought in the form $F(e) = u(e)G^2(e)$ where $u(e)$ is a linear function that assures that $F(e) \le 0$ in (35) and $G(e)$ is a function that maximizes the Fourier transform $\widehat{F}(0)$. In the univariate case it turns out that a good choice for G is a delta-function at (or near) d. An approximation of the delta-function is given by the (Dirichlet) kernel U_κ which is its projection on V_κ. We therefore seek to modify the operator S_κ so that U_κ becomes its eigenfunction with eigenvalue θ_κ, express the bound of Theorem 5.1 as a function of θ_κ and optimize on κ within the limits (35). The reader is referred to [7] for a more detailed discussion of these ideas.

Theorem 5.2. *Let κ be any degree such that $P(e) \le \lambda_{\kappa-1}$ for all shapes e with $|e|' \ge d$, where λ_i is the maximum eigenvalue of S_i and $d \ge 1$ is an integer.*

Let $C \subset \overrightarrow{H}$ be an (nr, M, d) code. Then

$$M \le \frac{4r\delta_{\text{crit}}(n-\kappa)(q^r-1)^\kappa}{\delta_{\text{crit}} rn - \lambda_\kappa}\binom{n}{\kappa}. \tag{38}$$

Let C be a $(t = d-1, n, r, q)$ OOA of size M. Then

$$M \ge \frac{q^{nr}}{\binom{n}{\kappa}} \frac{(\delta_{\text{crit}} rn - \lambda_\kappa)}{4r\delta_{\text{crit}}(n-\kappa)(q^r-1)^\kappa}. \tag{39}$$

Proof : Consider the operator T_κ that equals S_κ on $V_{\kappa-1}$ and acts on a function $\varphi \in V_\kappa \backslash V_{\kappa-1}$ by

$$T_\kappa(\varphi) := S_\kappa\varphi - \sum_{f:|f|=\kappa} \varepsilon_f \varphi_f \widetilde{K}_f,$$

where $\varepsilon_f > 0$ are some constants indexed by the partitions of weight κ (their values will be chosen later). The matrix of T_κ in the orthonormal basis equals

$$\widetilde{\mathbf{T}}_\kappa = \widetilde{\mathbf{S}}_\kappa - \begin{bmatrix} 0 & 0 \\ 0 & E \end{bmatrix}$$

where $E = \text{diag}(\varepsilon_f, |f| = \kappa)$ is a matrix of order $\binom{\kappa+r-1}{r-1}$. Let m be such that $\widetilde{\mathbf{T}}_\kappa + mI > 0$. By Perron-Frobenius [11, p. 80], the spectral radius $\rho(T_\kappa + mI)$ is well defined and is an eigenvalue of (algebraic and geometric) multiplicity one of $T_\kappa + mI$. Moreover, again using Perron-Frobenius,

$$\rho(S_{\kappa-1} + mI) < \rho(T_\kappa + mI) < \rho(S_\kappa + mI).$$

Then

$$\lambda_{\kappa-1} < \theta_\kappa < \lambda_\kappa \tag{40}$$

where $\theta_\kappa = \rho(T_\kappa)$. Let $G > 0$ be the eigenfunction of T_κ with eigenvalue θ_κ. Let us write out the product $P(e)G$ in the orthonormal basis:

$$P(e)G = S_\kappa G + G_\kappa A_\kappa \widetilde{\mathbb{K}}_{\kappa+1} = \theta_\kappa G + \sum_{f:|f|=\kappa} \varepsilon_f G_f \widetilde{K}_f + G_\kappa A_\kappa \widetilde{\mathbb{K}}_{\kappa+1}.$$

where G_κ is a projection of the vector G on the space $V_\kappa \backslash V_{\kappa-1}$. This implies the equality

$$G = \frac{\sum_{|f|=\kappa} G_f(\varepsilon_f \widetilde{K}_f + Q_f)}{P(e) - \theta_\kappa},$$

where $Q_f(x)$ is defined after (34). Now take $F(x) = (P(x) - \theta_\kappa)G^2(x)$. Let us verify (35). Since multiplication by a function is a self-adjoint operator, we obtain

$$F_0 = \langle F, 1\rangle = \langle \sum_{|f|=\kappa} G_f(\varepsilon_f \widetilde{K}_f + Q_f), G\rangle = \sum_{|f|=\kappa} G_f^2 \varepsilon_f > 0.$$

Using (24) one can easily check that $F_e \geq 0$ for all $e \neq 0$. The assumption of the theorem together with (40) implies that $F(f) \leq 0$ for $|f|' \geq d$. Hence

$$\begin{aligned} M &\leq \frac{F(0)}{F_0} \\ &= \frac{\Big(\sum_{|f|=\kappa} G_f(\varepsilon_f \widetilde{K}_f(0) + Q_f(0))\Big)^2}{(P(0) - \theta_\kappa)\sum_{|f|=\kappa} G_f^2 \varepsilon_f} \\ &\leq \frac{1}{P(0) - \lambda_\kappa} \sum_{|f|=\kappa} \frac{(\varepsilon_f \widetilde{K}_f(0) + Q_f(0))^2}{\varepsilon_f}, \end{aligned}$$

where in the last step we used the Cauchy-Schwarz inequality. Computing the minimum on ε_f, we obtain

$$M \leq \frac{4}{P(0) - \lambda_\kappa} \sum_{|f|=\kappa} Q_f(0)\sqrt{v_f}. \tag{41}$$

Next,

$$\sum_{|f|=\kappa} Q_f(0)\sqrt{v_f} = \sum_{f:|f|=\kappa} \sqrt{v_f} \sum_{h:|h|=\kappa+1} A_\kappa[f,h]\sqrt{v_h}.$$

Let $h = (f_1, \dots, f_i + 1, \dots, f_r)$ for some $i, 1 \leq i \leq r$. Then using (1) we find

$$\begin{aligned} A_\kappa[f,h]\sqrt{v_h} &= L_i\sqrt{(f_i+1)(n-\kappa)q^{i-1}(q-1)}\sqrt{v_h} \\ &= L_i\sqrt{(f_i+1)(n-\kappa)q^{i-1}(q-1)}\sqrt{v_f\frac{(n-\kappa)q^{i-1}(q-1)}{f_i+1}} \\ &= \Big(1 - \frac{1}{q^{r-i+1}}\Big)(n-\kappa)\sqrt{v_f}. \end{aligned}$$

Thus we have

$$\begin{aligned} \sum_{|f|=\kappa} Q_f(0)\sqrt{v_f} &= \sum_{|f|=\kappa}\sum_{i=1}^{r}(n-\kappa)\Big(1 - \frac{1}{q^{r-i+1}}\Big)v_f \\ &= (n-\kappa)r\delta_{\text{crit}} \sum_{|f|=\kappa} v_f = (n-\kappa)r\delta_{\text{crit}}\binom{n}{\kappa}(q^r-1)^\kappa. \end{aligned}$$

Substitution of this expression into (41) concludes the proof of (38). The bound (39) follows by (37). ∎

5-B. **Spectral radius of $\mathbf{S}_\kappa$.** In this section we derive an asymptotic lower bound on the spectral radius of $\mathbf{S}_\kappa$. This estimate will be later used to optimize the bound (38) on the choice of κ.

Theorem 5.3.

$$\lim_{\substack{n\to\infty\\ \frac{\kappa}{n}\to\tau}} \frac{\lambda_\kappa}{n} \ge \max_{\substack{\tau_i\ge 0\\ \sum_{i=1}^r \tau_i=\tau}} \Lambda(\tau_1,\dots,\tau_r),$$

where

$$\Lambda(\tau_1,\dots,\tau_r)=\sum_{i=1}^r L_i\Big(2\sqrt{(1-\tau)\tau_i(q-1)q^{i-1}} \\ +(q-2)\tau_i(q^r-q^{i-1})+2\frac{(q-1)}{q}\sum_{k=1}^{i-1}\sqrt{\tau_k\tau_i q^{i+k}}\Big). \tag{42}$$

To prove this theorem, we will bound below the largest eigenvalue λ_κ of the matrix $\widetilde{\mathbf{S}}_\kappa$. For any real vector y we have

$$\lambda_\kappa \ge \frac{y^T\widetilde{\mathbf{S}}_\kappa y}{(y,y)}.$$

We will construct a suitable $(0,1)$-vector y. Its coordinates are indexed by the partitions arranged in the increasing order of their length μ and lexicographically within a block of coordinates for each value of $\mu, 0\le\mu\le\kappa$. Let $y=(y_0,y_1,\dots,y_\kappa)$ where $y_\mu=(y_f,|f|=\mu)$.

Let $f, |f|=\mu$, be a shape vector. For an integer J consider the set

$$\mathcal{F}_\mu=\mathcal{F}_\mu(J,f)\triangleq\{(f_1+\mu-\kappa+j_1,\dots,f_r+j_r):\sum_{i=1}^r j_i=0;\ |j_i|\le J, i=1,\dots,r\}$$

and denote $m=|\mathcal{F}_\mu|$. Next, let

$$(y_\mu)_h=1(h\in\mathcal{F}_\mu)$$

for $\mu=\kappa+1-s,\dots,\kappa$ where s will be chosen later, and $y_\mu=0$ otherwise.

In the next two lemmas we derive a lower bound on the part of the product $y^T\widetilde{\mathbf{S}}_\kappa y$ that involves only the rows of $\widetilde{\mathbf{S}}_\kappa$ that correspond to the shapes f of length μ. Let

$$E_h=\{(h_1,\dots,h_k\pm 1,\dots,h_l\mp 1,\dots,h_r), 1\le k<l\le r\}$$

be the index set of the nonzero off-diagonal elements in the row in B_μ which is indexed by $h=(h_1,\dots,h_r)$.

Lemma 5.4. *Let* $e=\operatorname{argmin}_{h\in\mathcal{F}_\mu}(\sum_{g\in E_h\cup\{h\}}B_\mu[h,g])$ *and let* $\psi_\mu=\sum_g B_\mu[e,g]$. *Then*

$$y_\mu^T B_\mu y_\mu \ge \psi_\mu m(1-o_m(1)).$$

Proof : I. Since $|h|=\mu$ for every $h\in\mathcal{F}_\mu$, the quantity $|\mathcal{F}_\mu|$ equals the number of ordered partitions of 0 into at most r parts, each part bounded between $-J$ and J, or the number of ordered partitions

$$Jr=\sum_{i=1}^r j_i,\quad 0\le j_i\le 2J,\ i=1,\dots,r.$$

The number of such partitions is given by [17, p. 1037]:

$$\pi(r,2J,Jr)=\sum_{i=0}^{\lfloor\frac r2\rfloor}(-1)^i\binom{r}{i}\binom{r+Jr-(2J+1)i-1}{r-1}.$$

Writing this expression as a polynomial in J, we find the coefficient of J^{r-1} to be

$$\frac{1}{(r-1)!}\sum_{i=0}^{\lfloor\frac r2\rfloor}(-1)^i\binom{r}{i}(r-2i)^{r-1}.$$

Since this is always positive[1], we conclude that m is a degree-$(r-1)$ polynomial in J; in particular, if $J\to\infty$, then also $m\to\infty$.

II. We have

$$y_\mu^T B_\mu y_\mu=\sum_{h,g\in\mathcal{F}_\mu}B_\mu[h,g].$$

To bound $y_\mu^T B_\mu y_\mu$ below we estimate the difference between the above sum and the sum of all the nonzero elements of B_μ in the rows $h\in\mathcal{F}_\mu$ which is obtained by replacing the range of column indices g above with $g\in E_h\cup\{h\}$. Therefore, for a given $h\in\mathcal{F}_\mu$ let us estimate the number $|E_h\backslash\mathcal{F}_\mu|$ of nonzero entries in $B_\mu[h,\cdot]$ not included in the sum. Let $f=(f_1,\dots,f_r)$ and let h be of the form $h=(\dots,f_k+J,\dots)\in\mathcal{F}_\mu$ for some $1\le k\le r$. Consider the column indices $g\in E_h$ given by

$$g=(f_1+\mu-\kappa+j_1,\dots,f_k+J+1,\dots,f_l+j_l-1,\dots,f_r+j_r) \tag{43}$$

for any $k\ne l\in\{1,\dots,r\}$. For any pair h,g of this form, $B_\mu[h,g]\ne 0$ but $g\notin\mathcal{F}_\mu$. The number of shapes h that result in shapes g of the form (43) equals the number of ordered partitions of $-J$ into at most $r-1$ parts of magnitude $\le J$; equivalently, this is the number of ordered partitions

$$J(r-2)=j_2+\dots+j_r,\quad 0\le j_i\le 2J, i=2,\dots,r,$$

which equals $\Pi_+\triangleq\pi(r-1,2J,J(r-2))$.

Next consider the row indices $h=(\dots,f_k-J,\dots)\in\mathcal{F}_\mu$ and column indices $g\in E_h$ given by

$$g=(f_1+\mu-\kappa+j_1,\dots,f_k-J-1,\dots,f_l+j_l+1,\dots,f_r+j_r)$$

which again account for $B_\mu[h,g]\ne 0$ and $g\notin\mathcal{F}_\mu$. The number of such shapes h equals the number of ordered partitions of Jr into $r-1$ or fewer parts $0\le j_i\le 2J$. Denote this number by $\Pi_-\triangleq\pi(r-1,2J,Jr)$. Note that as $J\to\infty$, both Π_+ and Π_- grow proportionally to J^{r-2}.

It is easy to verify that $E_h\backslash\mathcal{F}_\mu\ne\emptyset$ if and only if h and g are of the described form. Observe that by (30), $|E_f|=r^2-r$. We then obtain

$$\sum_{h,g\in\mathcal{F}_\mu}B_\mu[h,g]\ge\psi_\mu(m-r(r^2-r)(\Pi_++\Pi_-))=\psi_\mu m(1-o_m(1)).$$

The lemma is proved. ∎

[1] To prove positivity, observe that the numbers $S_{r,m}=\sum_{i=0}^{\lfloor\frac r2\rfloor}(-1)^i\binom{r}{i}(r-2i)^m$ satisfy the recurrence

$$S_{r,m}=r^2S_{r,m-2}+4r(r-1)S_{r-2,m-2},\quad 3\le m\le r-1$$

and then use induction to prove that $S_{r.m}>0$ (<0) according as $r-m\equiv 1$ or 3 mod 4.

We now consider the part of the product $y^T\widetilde{\mathbf{S}}_\kappa y$ that involves the matrix $C_\mu, \mu = \kappa - s+2,\dots,\kappa$. For a shape h let

$$D_h = \{(h_1,\dots,h_k-1,\dots,h_r), 1 \le k \le r\}.$$

The proof of the next lemma is very similar to the above proof and will therefore be omitted.

Lemma 5.5. *Let* $e = \operatorname{argmin}_{h\in\mathcal{F}_\mu}(\sum_{g\in D_h} C_\mu[h,g])$ *and let* $\phi_\mu = \sum_g C_\mu[e,g]$.

$$y_\mu^T C_\mu y_{\mu-1} \ge \phi_\mu m(1-o_m(1)).$$

To complete the proof of Theorem 5.3, compute

$$\begin{aligned}
\lambda_\kappa &\ge \frac{1}{ms} y^T S_\kappa y \\
&= \frac{1}{ms}\Big(\sum_{\mu=\kappa+1-s}^{\kappa} y_\mu^T B_\mu y_\mu + 2\sum_{\mu=\kappa+2-s}^{\kappa} y_\mu^T C_\mu y_{\mu-1}\Big) \\
&\ge \frac{1}{s}\Big(\sum_{\mu=\kappa+1-s}^{\kappa}\psi_\mu + 2\sum_{\mu=\kappa+2-s}^{\kappa}\phi_\mu\Big)(1-o_m(1)) \\
&\ge \psi^* + 2\frac{s-1}{s}\phi^*(1-o_m(1)),
\end{aligned}$$

where ψ^* (ϕ^*) is the smallest of the numbers ψ_μ (ϕ_μ) above. Note that both ψ^* and ϕ^* are nonzero. Now let $n\to\infty, \kappa = \tau n$, and let us choose f in the definition of $\mathcal{F}_\mu$ to be of the form $f = (f_1,\dots,f_r), f_i = n\tau_i, 1\le i\le r$. We assume that none of the τ_i's approach 0 as n grows. Take $s = o(n), s\to\infty$. Using (30), and letting $J = o(n), J\to\infty$ we get

$$\lim_{n\to\infty}\frac{\psi^*}{n} = \sum_{i=1}^r L_i\Big((q-2)\tau_i(q^r-q^{i-1}) + 2\frac{(q-1)}{q}\sum_{k=1}^{i-1}\sqrt{\tau_k\tau_i q^{i+k}}\Big)$$

$$\lim_{n\to\infty}\frac{\phi^*}{n} = \sum_{i=1}^r L_i\sqrt{(1-\tau)\tau_i(q-1)q^{i-1}}.$$

Then since $\kappa/n\to\tau$,

$$\lim_{n\to\infty}\frac{\lambda_\kappa}{n} \ge \lim_{n\to\infty}\frac{y^T S_\kappa y}{msn} \ge \Lambda(\tau_1,\dots,\tau_r).$$

The theorem is proved.

5-C. **Asymptotic estimate for codes and OOAs.** Theorems 5.2 and 5.3 together enable us to prove one of the main results of the paper.

Theorem 5.6. *Let* $R_{\text{LP}}(\delta)$ *be the function defined parametrically by the relations*

$$R(\tau) = \frac{1}{r}\left(h_q(\tau) + \tau\log_q\frac{q^r-1}{q-1}\right) \tag{44}$$

$$\delta(\tau) = \delta_{\text{crit}} - \frac{1}{r}\max_{\substack{\tau_i\ge 0\\ \sum_{i=1}^r\tau_i=\tau}}\Lambda(\tau_1,\dots,\tau_r), \quad 0\le\tau\le 1. \tag{45}$$

Then the asymptotic rate of any code family of relative distance δ *satisfies* $R\le R_{\text{LP}}(\delta)$ *and the rate of any family of OOAs of relative strength* δ *satisfies* $R \ge 1-R_{\text{LP}}(\delta)$.

To prove this theorem, take the logarithms in (38) and pass to the limit as $n \to \infty$. Using the standard asymptotics for the binomial coefficient, we find that the code rate is bounded above by the right-hand side of (44). The condition $P(e) \le \lambda_{\kappa-1}$ of the Theorem 5.2 will be satisfied for large n if

$$\delta_{\text{crit}} - \delta \le \frac{\lambda_{\tau n}}{rn}.$$

This defines the function in (45). Thus, the proof is complete.

Remark. For $r = 1$ this bound reduces to the linear programming bound on the rate of codes in [2]. Just as that result, the bound of this theorem improves upon the asymptotic Plotkin bound for large values of the code distance.

6. The Case $r = 2$

In this section we prove a bound for codes in $\mathcal{Q}^{2,n}$ which improves upon the general result of the previous section. The improvement is due to the fact that in the case $r = 2$ it is possible to work with the polynomials $K_f(e)$ in their explicit form, and base the bound on the behavior of their zeros instead of the spectral radius of the operator S_κ. Namely, let $f = (f_1, f_2), e = (e_1, e_2)$. From (32) we have

$$K_f(e) = q^{f_2} k_{f_2}(n - e_2, e_1) k_{f_1}(n - f_2, e_2).$$

We also have

$$P(e) = n\Big(2 - \frac{q+1}{q^2}\Big) - e_1 - 2e_2.$$

We will use the following properties of the polynomials k_s whose proofs are found for instance in [21]. Let $x_i(n,s), i = 1, \dots, s$ be the roots of k_s in the ascending order. Then

$$x_i(n-1,s) < x_i(n,s) < x_i(n-1,s-1) < x_i(n,s-1) < x_{i+1}(n,s), \\ 1 < s < n,\ i = 1, \dots, s-1. \tag{46}$$

Let $n \to \infty, s/n \to y$. Then

$$\lim_{n\to\infty} \frac{x_1(n,s)}{n} = \gamma(y) \triangleq \frac{q-1}{q} - \frac{q-2}{q} y - \frac{2}{q}\sqrt{(q-1)y(1-y)}. \tag{47}$$

The Krawtchouk polynomials satisfy the recurrence

$$k_s(n,x) = k_s(n-1,x) + (q-1)k_{s-1}(n-1,x) \tag{48}$$

and a Christoffel-Darboux formula of the form (34)

$$q(x-y)\sum_{s=0}^{h} \frac{k_s(x)k_s(y)}{k_s(0)} = \frac{h+1}{k_h(0)}(k_{h+1}(y)k_h(x) - k_{h+1}(x)k_h(y)). \tag{49}$$

Remark: Properties (46)-(49) are usually stated for integer n. This is related to the fact that the polynomials $k_s(n,x)$ represent the eigenvalues of the Hamming association scheme. As pointed out to us by M. Aaltonen [3], it is possible to prove these properties for any $n \in \mathbb{R}^+$ relying on the generating function of the Krawtchouk polynomials.

The main result of this section is given in the following theorem.

Theorem 6.1. *The asymptotic rate of any family of codes of relative distance δ satisfies $R \le \Phi(\delta)$, where*

$$\Phi(\delta) = \min_{\tau_1,\tau_2} {}^1\!/_2 \Big\{\tau_2 + h_q(\tau_1) + (1-\tau_1)h_q\Big(\frac{\tau_2}{1-\tau_1}\Big)\Big\},$$

where the minimum is taken over all τ_1, τ_2 *that satisfy*

$$0 \le \tau_1 \le (q-1)/q^2, \quad 0 \le \tau_2 \le (q-1)/q,$$
$$\gamma(\tau_2) + (2-\gamma(\tau_2))(1-\tau_2)\gamma(\tau_1) \le 2\delta.$$

The asymptotic rate of any family of OOAs of relative strength δ *satisfies* $R \ge 1 - \Phi(\delta)$.

The remainder of the section is devoted to the proof of this result. We note that the polynomials $K_f(e)$ are formed as products of two Krawtchouk polynomials. A similar situation arose in [1] which dealt with the Johnson association scheme whose (second) eigenvalues are equal to a product of a Krawtchouk and a Hahn polynomial. Therefore, we adopt some elements of the analysis in [1] in our proof below.

In quest of an LP bound, we require a polynomial $F(e) = F(e_1, e_2)$ that satisfies conditions (35). Consider the polynomial of the form

$$F(e) = (P(e) - P(a))(U_L(a,e))^2 \tag{50}$$

for some $a = (\alpha, \beta)$ and a subset L. For brevity below we write S_{fh} instead of $\mathbf{S}_\kappa[f,h]$ and denote $\bar{L} = \Delta_{2,n} \backslash L$. We find

$$\begin{aligned} F_0 = \langle F, 1\rangle &= \langle (P(e)-P(a))U_L(a,e), U_L(a,e)\rangle \\ &= \langle \sum_{f\in L} \frac{1}{v_f} \sum_{h\in\bar{L}} S_{fh}(-K_h(a))K_f(e), U_L\rangle \\ &= -\sum_{f\in L}\sum_{h\in\bar{L}} S_{fh}K_h(a)\frac{K_f(a)}{v_f}. \end{aligned}$$

In order to ensure that $F_0 > 0$ we will choose L and a so that

$$K_h(a) \le 0 \quad \text{if } h \in \bar{L}; \qquad K_f(a) > 0 \quad \text{if } f \in L. \tag{51}$$

Let $s = (s_1 - 1, s_2) \in \Delta_{2,n}$ be a shape that satisfies $\{(s_1-1, s_2+1), (s_1, s_2)\} \subset \Delta_{2,n}$. Let $a = (\alpha, \beta)$ satisfy

$$\beta = x_1(n-s_2, s_1), \quad x_1(n-\beta, s_2+1) < \alpha < x_1(n-\beta, s_2), \quad \alpha + 2\beta \le d. \tag{52}$$

For any $f_2, 0 \le f_2 \le s_2 + 1$ denote by $\phi(f_2)$ the degree such that

$$x_1(n-f_2, \phi(f_2)+1) \le \beta < x_1(n-f_2, \phi(f_2)). \tag{53}$$

By (46), $\phi(\cdot)$ is well defined and implies the following:

$$[(x_1(n-u,w) > \beta) \ \Rightarrow\ (w \le \phi(u))], \quad [(x_1(n-u,w) \le \beta) \ \Rightarrow\ (w \ge \phi(u)+1)].$$

We choose the region L to be given by

$$L = (f_1, f_2 : f_2 = 0, \dots, s_2; f_1 = 0, \dots, \phi(f_2)).$$

For the moment this choice is not unique because there are many possibilities for s. This ambiguity will be later removed by optimizing the bound on the choice of s.

To argue about the sign of F_0 we need to establish some properties of the region L. First, we claim that for a fixed f_2,

$$\phi(f_2) - 1 \le \phi(f_2+1) \le \phi(f_2). \tag{54}$$

Indeed, by (46),

$$\beta < x_1(n-f_2, \phi(f_2)) < x_1(n-f_2-1, \phi(f_2)-1)$$

which implies the left-hand side of (54). On the other hand,

$$\beta \ge x_1(n-f_2, \phi(f_2)+1) > x_1(n-f_2-1, \phi(f_2)+1)$$

which implies the right-hand side.

The values of f, h for which $S_{fh} \neq 0$ are given in (30). In particular, if $f \in L$, then the set H of the shape vectors h that index the nonzero matrix elements of **S** and that lie outside the region L is as follows:

$$H = \{(\phi(f_2)+1, f_2), f_2 = 0, 1, \dots, s_2\} \cup \{(f_1, s_2+1), f_1 = 0, 1, \dots, s_1 - 1\}.$$

The region L and the corresponding set H are shown in Fig. 1. By our choice of the parameters,

$$\begin{aligned} k_{f_2}(n-\beta, \alpha) &> 0 \qquad (0 \le f_2 \le s_2), \\ k_{s_2+1}(n-\beta, \alpha) &< 0, \\ k_{f_1}(n-f_2, \beta) &> 0 \qquad (0 \le f_1 \le \phi(f_2),\ 0 \le f_2 \le s_2+1), \\ k_{\phi(f_2)+1}(n-f_2, \beta) &\le 0 \qquad (0 \le f_2 \le s_2+1). \end{aligned}$$

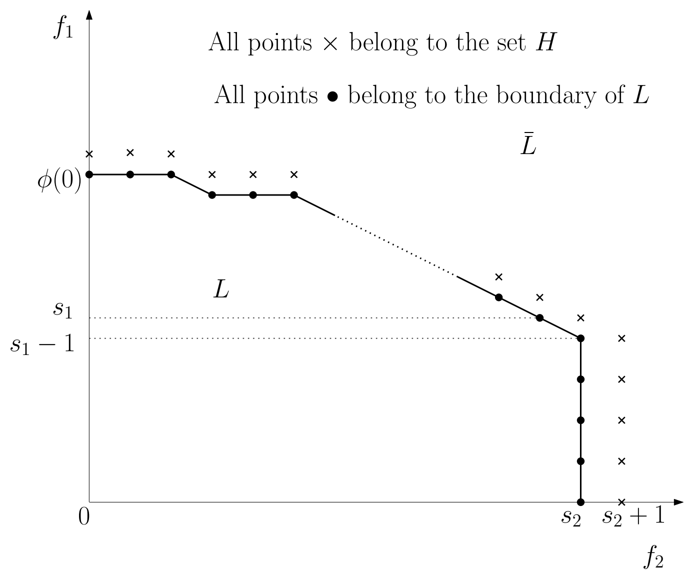

FIGURE 1. The region L

Then

$$K_{(f_1,f_2)}(a) = q^{f_2} k_{f_2}(n-\beta,\alpha) k_{f_1}(n-f_2,\beta) > 0, \quad f \in L, \tag{55}$$

$$K_{(\phi(f_2)+1,f_2)}(a) = q^{f_2} k_{f_2}(n-\beta,\alpha) k_{\phi(f_2)+1}(n-f_2,\beta) \le 0, \quad 0 \le f_2 \le s_2, \tag{56}$$

$$K_{(f_1,s_2+1)}(a) = q^{s_2+1} k_{s_2+1}(n-\beta,\alpha) k_{f_1}(n-s_2-1,\beta) < 0, \quad 0 \le f_1 \le s_1 - 1. \tag{57}$$

Thus,

$$K_f(a) \le 0 \ \ (f \in \bar{L}), \quad K_f(a) > 0 \ \ (f \in L). \tag{58}$$

This proves that $F_0 > 0$.

Let us show that $F_e \ge 0$ for all e. For this rewrite F as follows:

$$\begin{aligned}
F(e) &= ((P(e)-P(a))U_L(a,e)^2 \\
&= \sum_{f\in L}\frac{1}{v_f}\sum_{h\in\bar L} S_{fh}(K_h(e)K_f(a)-K_h(a)K_f(e))\sum_{g\in L}\frac{K_g(a)K_g(e)}{v_g} \\
&= \Big(\sum_{h\in\bar L}K_h(e)\sum_{f\in L}\frac{S_{fh}K_f(a)}{v_f}-\sum_{f\in L}K_f(e)\sum_{h\in\bar L}\frac{K_h(a)S_{fh}}{v_f}\Big)\sum_{g\in L}\frac{K_g(a)K_g(e)}{v_g} \\
&= \sum_{h\in\bar L,\; g\in L}\frac{K_g(a)}{v_g}K_h(e)K_g(e)\sum_{f\in L}\frac{S_{fh}K_f(a)}{v_f} \\
&\qquad\qquad -\sum_{f,g\in L}\frac{K_g(a)}{v_g}K_f(e)K_g(e)\sum_{h\in\bar L}\frac{K_h(a)S_{fh}}{v_f}.
\end{aligned}$$

By (24), the products K_hK_g and K_fK_g are expanded in the basis $\{K_f\}$ with nonnegative coefficients. Moreover, the other terms in the above formula also have the needed signs on account of (55)-(57). This establishes our claim.

Finally, because of the third condition in (52), $F(e)\le 0$ for all e with $|e|'\ge d$.

We are now able to formulate the bound on codes and OOAs.

Theorem 6.2. *Let C be an $(2n,M,d)$ code $C\subset \overrightarrow{H}(q,n,2)$. Then*

$$M\le \frac{4(n-\beta-s_2)(n-s_2-s_1+1)^2(q-1)^3(\alpha+2\beta)}{q^3\alpha^2\beta^2}v_s, \tag{59}$$

where $s=(s_1-1,s_2)$ satisfies $\{(s_1-1,s_2+1),(s_1,s_2)\}\subset\Delta_{2,n}$ and $a=(\alpha,\beta)$ is chosen to fulfill conditions (52).

Let C be a $(t=d-1,n,2,q)$ OOA of size M. Then

$$M\ge \frac{q^{nr}}{v_s}\frac{q^3\alpha^2\beta^2}{4(n-\beta-s_2)(n-s_2-s_1+1)^2(q-1)^3(\alpha+2\beta)}. \tag{60}$$

Proof : Let us compute $F_0=\langle F,1\rangle$. Denote $\sigma_1=(s_1-1,s_2+1), \sigma_2=(s_1-2,s_2+1)$. By (58) and (26) we have

$$\begin{aligned}
F_0 &= -\sum_{f\in L}\frac{K_f(a)}{v_f}\sum_{h\in\bar L}S_{fh}K_h(a) \\
&\ge -\frac{K_s(a)}{v_s}(S_{s,\sigma_1}K_{\sigma_1}(a)+S_{s,\sigma_2}K_{\sigma_2}(a)+S_{s,(s_1,s_2)}K_{(s_1,s_2)}(a)) \\
&= -\frac{K_s(a)}{q^2v_s}\Big((s_2+1)K_{\sigma_1}(a)+(s_2+1)(q-1)K_{\sigma_2}(a)+s_1(q+1)K_{(s_1,s_2)}(a)\Big) \\
&= -\frac{K_s(a)(s_2+1)q^{s_2+1}}{q^2v_s}k_{s_2+1}(n-\beta,\alpha)k_{s_1-1}(n-s_2,\beta). \qquad (61)
\end{aligned}$$

Let us now evaluate $U_L(a,0)$.

$$U_L(a,0)=\sum_{f\in L}K_f(a)=\sum_{f_2=0}^{s_2}q^{f_2}k_{f_2}(n-\beta,\alpha)\sum_{f_1=0}^{\phi(f_2)}k_{f_1}(n-f_2,\beta).$$

Let us bound above the last sum. We shall prove that

$$\sum_{f_1=0}^{\phi(f_2)}k_{f_1}(n-f_2,\beta)\le q^{s_2-f_2}\sum_{f_1=0}^{\phi(s_2)}k_{f_1}(n-s_2,\beta). \tag{62}$$

Indeed, using (48), we obtain

$$\sum_{f_1=0}^{\phi(f_2)} k_{f_1}(n-f_2,\beta) = \sum_{f_1=0}^{\phi(f_2)} (k_{f_1}(n-f_2-1,\beta) + (q-1)k_{f_1-1}(n-f_2-1,\beta))$$
$$= k_{\phi(f_2)}(n-f_2-1,\beta) + q\sum_{f_1=0}^{\phi(f_2)-1} k_{f_1}(n-f_2-1,\beta).$$

Recall that $\phi(f_2+1)=\phi(f_2)$ or $\phi(f_2+1)=\phi(f_2)-1$. In the former case,

$$k_{\phi(f_2)}(n-f_2-1,\beta) + q\sum_{f_1=0}^{\phi(f_2)-1} k_{f_1}(n-f_2-1,\beta) \le q\sum_{f_1=0}^{\phi(f_2+1)} k_{f_1}(n-f_2-1,\beta);$$

in the latter, $k_{\phi(f_2)}(n-f_2-1,\beta) = k_{\phi(f_2+1)+1}(n-f_2-1,\beta)\le 0$ on account of (53) and (46). Repeating this procedure s_2-f_2 times, we arrive at (62).

Note that $\phi(s_2)=s_1-1$. Therefore

$$U_L(a,0) \le q^{s_2}\sum_{f_2=0}^{s_2} k_{f_2}(n-\beta,\alpha)\sum_{f_1=0}^{s_1-1} k_{f_1}(n-s_2,\beta).$$

By (49), (52), and (23) we have

$$\sum_{f_1=0}^{s_1-1} k_{f_1}(n-s_2,\beta) = \frac{s_1\binom{n-s_2}{s_1}(q-1)}{q\beta\binom{n-s_2}{s_1-1}} k_{s_1-1}(n-s_2,\beta),$$

$$\sum_{f_2=0}^{s_2} k_{f_2}(n',\alpha) = \frac{(s_2+1)(k_{s_2+1}(n',0)k_{s_2}(n',\alpha) - k_{s_2+1}(n',\alpha)k_{s_2}(n',0))}{q\alpha k_{s_2}(n',0)}$$
$$= \frac{s_2+1}{q\alpha} k_{s_2}(n',\alpha)(W(0)-W(\alpha)),$$

where $n'=n-\beta$ and $W(x)=k_{s_2+1}(n',x)/k_{s_2}(n',x)$. Using these expressions, we can bound $U_L(a,0)$ as

$$U_L(a,0) \le \frac{(s_2+1)(n-s_2-s_1+1)(q-1)}{q^2\alpha\beta} K_s(a)(W(0)-W(\alpha)).$$

Hence using (36), (50), and (61) we can write

$$M \le v_s \frac{(s_2+1)(n-s_2-s_1+1)^2(q-1)^2(\alpha+2\beta)}{q^3\alpha^2\beta^2}\frac{(W(0)-W(\alpha))^2}{-W(\alpha)}.$$

Since $W(0)=(q-1)(n'-s_2)/(s_2+1)>0>W(\alpha)>-\infty$ as α ranges in between the bounds in (52), it is possible to find α such that $W(\alpha)=-W(0)$. With this choice and (1) the last expression turns into (59). The estimate (60) follows from (37). ∎

The proof of Theorem 6.1 is obtained by passing to asymptotics in (59). Namely, let $n\to\infty, d/nr\to\delta, s_1/n\to\tau_1, s_2/n\to\tau_2$. By (47),

$$\limsup_{n\to\infty}\frac{\beta}{n} = \gamma(\tau_1)(1-\tau_2), \quad \limsup_{n\to\infty}\frac{\alpha}{n} = \gamma(\tau_2)(1-\gamma(\tau_1)(1-\tau_2)).$$

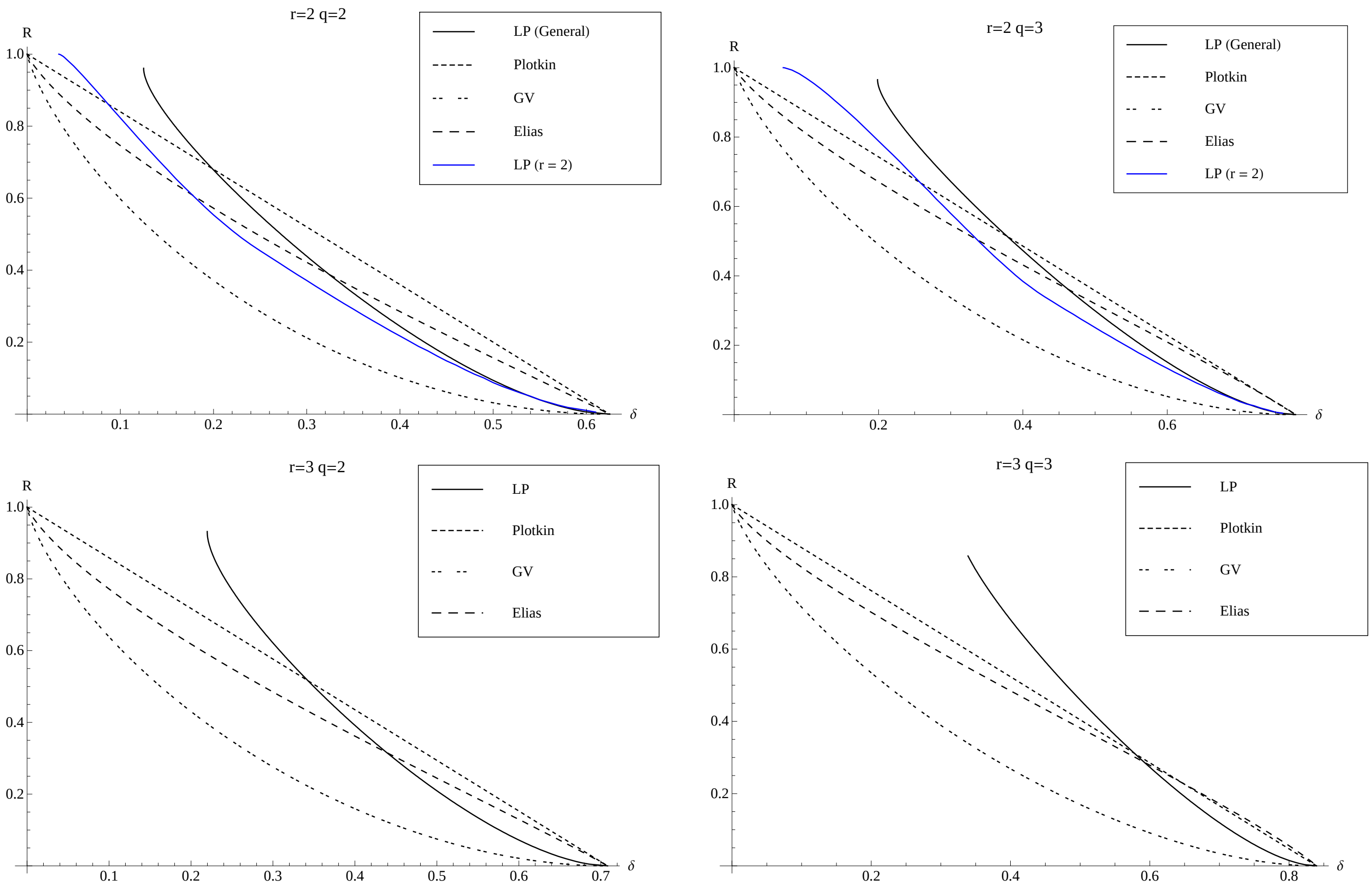

FIGURE 2. Bounds for codes.

Computing the logarithm on the right-hand side of (59), we observe that the only term of exponential growth arises from v_s. Using standard estimates we obtain

$$\begin{aligned}\log_q v_s &= \log_q \binom{n}{s_1-1}\binom{n-s_1+1}{s_2} q^{s_2}(q-1)^{s_1+s_2-1}\\ &\le n\Big\{\tau_2 + h_q(\tau_1) + (1-\tau_1)h_q\big(\frac{\tau_2}{1-\tau_1}\big)\Big\}.\end{aligned}$$

The tightest bound is obtained by computing the minimum of this expression on τ_1, τ_2. The range of the variables τ_1, τ_2 is obtained on observing that $n(q-1)/q^2$ and $n(q-1)/q$ are the maximizing values of s_1, s_2 for large n (by a direct calculation from the above expression; or, specializing from a general result in [34]). The third restriction in the statement of the theorem is implied by $\alpha + 2\beta \le d$. This completes the proof.

Asymptotic bounds for ordered codes are shown in several plots in Fig. 2.

Remark. The NRT metric is an example of a wide class of metrics on the set $\mathcal{Q}^N$ termed poset metrics following Brualdi et al. [12]. To define a poset metric, consider a partial order $P_\prec$ on the set $[1, 2, \ldots, N]$. An *ideal* in the order is a subset closed under the $\prec$ relation.

The $P_{\prec}$-weight of a vector $\boldsymbol{x} \in \mathcal{Q}^N$ is the size of the smallest ideal that contains the nonzero entries of $\boldsymbol{x}$. For instance, for the NRT weight, the relation $\prec$ can be defined as $(i_1, j_1) \prec (i_2, j_2)$ iff $i_1 = i_2, j_1 < j_2$, where i_1, i_2 are the indices of the block. A *dual order* $P_{\succ}$ is formed of the same set of chains as the order $P_{\prec}$ but with the signs reversed within each chain. In [24, 35, 14], and in our paper, the poset duality is realized as the $C \subset \overrightarrow{H}, C^{\perp} \subset \overleftarrow{H}$ convention. One of the main questions that arises in this context is to characterise the association scheme that arises from the order and in particular, to derive the MacWilliams-type relations. Partial orders that give rise to a univariate MacWilliams relation have been described by Kim and Oh [19]. On the other hand, rather little is known about the multivariate case of which the NRT space is an instance.

ACKNOWLEDGMENT: A.B. is grateful to William Martin for calling his attention to the problem of code bounds for the NRT space. The authors are also grateful to M. Aaltonen for a useful discussion of his work [1].

REFERENCES

[1] M. Aaltonen, *A new upper bound on nonbinary block codes*, Discrete Mathematics **83** (1990), no. 2-3, 139–160.
[2] ———, *Linear programming bounds for tree codes*, IEEE Trans. Inform. Theory **25** (1977), 85–90.
[3] ———, personal communication (2007).
[4] C. Bachoc, *Linear programming bounds for codes in Grassmannian spaces*, IEEE Trans. Inform. Theory **52** (2006), 2111–2126.
[5] E. Bannai and T. Ito, *Algebraic combinatorics I. Association schemes*, Benjamen/Cummings, London e. a., 1984.
[6] A. Barg and D. Nogin, *Spectral approach to linear programming bounds on codes*, Problems of Information Transmission **42** (2006), 12–25.
[7] ———, A functional view of upper bounds on codes, in Y. Li et al., Eds., *Coding and Cryptology*, Singapore: World Scientific (2008), pp. 15-24.
[8] J. Bierbrauer, Y. Edel, and W. Ch. Schmid, *Coding-theoretic constructions of (t, m, s)-nets and ordered orthogonal arrays*, J. Combin. Des. **10** (2002), no. 6, 403–418.
[9] J. Bierbrauer and W. Ch. Schmid, *An asymptotic Gilbert-Varshamov bound for (T, M, S)-nets*, Integers **5** (2005), no. 3, A4, 11 pp. (electronic).
[10] J. Bierbrauer, *A direct approach to linear programming bounds*, Des. Codes Cryptogr. **42** (2007), 127–143.
[11] A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance-regular graphs*, Springer-Verlag, Berlin e. a., 1989.
[12] R. A. Brualdi, J.S. Graves, and K. M. Lawrence, *Codes with a poset metric*, Discrete Math. **147** (1995), no. 1-3, 57–72.
[13] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Research Repts Suppl. **10** (1973), 1–97.
[14] S. T. Dougherty and M. M. Skriganov, *MacWilliams duality and the Rosenbloom-Tsfasman metric*, Mosc. Math. J. **2** (2002), no. 1, 81–97, 199.
[15] C. P. Dunkl and Y. Xu, *Orthogonal polynomials of several variables*, Cambridge University Press, 2001.
[16] A. Ganesan and P. O. Vontobel, *On the existence of universally decodable matrices*, IEEE Trans. Inform. Theory **53** (2007), no. 7, 2572–2575.
[17] I. M. Gessel and R. P. Stanley, *Algebraic enumeration*, Handbook of combinatorics, Vol. 2, Elsevier, Amsterdam, 1995, pp. 1021–1061.
[18] C. D. Godsil, *Algebraic combinatorics*, Chapman & Hall, New York, 1993.
[19] H. K. Kim and D. Y. Oh, *A classification of posets admitting MacWilliams identity*, IEEE Trans. Inform. Theory **51** (2005), 1424–1431.
[20] K. M. Lawrence, *A combinatorial characterization of (t, m, s)-nets in base b*, J. Combin. Designs **4** (1996), 275–293.
[21] V. I. Levenshtein, *Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces*, IEEE Trans. Inform. Theory **41** (1995), no. 5, 1303–1321.
[22] W. J. Martin, *Linear programming bounds for ordered orthogonal arrays and (T, M, S)-nets*, Monte Carlo and quasi-Monte Carlo methods 1998 (Claremont, CA), Springer, Berlin, 2000, pp. 368–376.

[23] ———, *(t, m, s)-nets*, Handbook of Combinatorial Designs (C. J. Colbourn and J. H. Dinitz, eds.), CRC Press, Boca Raton, FL, 2006, pp. 639–643.

[24] W. J. Martin and D. R. Stinson, *Association schemes for ordered orthogonal arrays and (T, M, S)-nets*, Canad. J. Math. **51** (1999), no. 2, 326–346.

[25] ———, *A generalized Rao bound for ordered orthogonal arrays and (t, m, s)-nets*, Canad. Math. Bull. **42** (1999), no. 3, 359–370.

[26] W. J. Martin and T. I. Visentin, *A dual Plotkin bound for (T, M, S)-nets*, IEEE Trans. Inform. Theory **53** (2007), no. 1, 411–415.

[27] J. L. Massey and S. Serconek, *Linear complexity of periodic sequences: A general theory*, "Advances in Cryptology" (CRYPTO '96), Lecture Notes in Comput. Sci., vol. **1109**, Springer, Berlin, 1996, pp. 358–371.

[28] G. L. Mullen and W. Ch. Schmid, *An equivalence between (t, m, s)-nets and strongly orthogonal hypercubes*, Journal of Combin. Theory, Ser. A **76** (1996), 164–174.

[29] H. Niederreiter, *Low-discrepancy point sets*, Monatsh. Math. **102** (1986), no. 2, 155–167.

[30] ———, *Digital nets and coding theory*, Coding Theory, Cryptography, and Combinatorics (K. Feng, H. Niederreiter, and C. Xing, eds.), Birkhäuser, Basel e.a., 2004, pp. 247–257.

[31] H. Niederreiter and C. Xing, *Rational points on curves over finite fields*, Cambridge University Press, 2001.

[32] R. R. Nielsen, *A class of Sudan-decodable codes*, IEEE Trans. Inform. Theory **46** (2000), no. 4, 1564–1572.

[33] B. Roos, *Multinomial and Krawtchouk approximations to the generalized multinomial distribution*, Theory Probab. Appl. **46** (2002), no. 1, 103–117

[34] M. Yu. Rosenbloom and M. A. Tsfasman, *Codes for the m-metric*, Problems of Information Transmission **33** (1997), no. 1, 45–52.

[35] M. M. Skriganov, *Coding theory and uniform distributions*, Algebra i Analiz **13** (2001), no. 2, 191–239, English translation in *St. Petersburg Math. J.* vol. 13 (2002), no. 2, 301–337.

[36] I. M. Sobol, *Distribution of points in a cube and approximate evaluation of integrals*, Ž. Vyčisl. Mat. i Mat. Fiz. **7** (1967), 784–802.

[37] M. V. Tratnik, *Multivariable Meixner, Krawtchouk, and Meixner-Pollaczek polynomials*, J. Math. Phys. **30** (1989), no. 12, 2740–2749.